504-REN-96/005
CSC10031825

MISSION OPERATIONS AND DATA SYSTEMS DIRECTORATE

Renaissance Standards

Version 2.0

May 1996

National Aeronautics and
Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

Renaissance Standards

Version 2.0

May 1996

Prepared Under Contract NAS5-31000
Task Assignment 86-601

Approved By:

Gary F. Meyers Date
Systems Engineering Office, Code 504

Goddard Space Flight Center
Greenbelt, Maryland

Preface

This document was developed by the Renaissance Team Systems Engineering Working Group of the Systems Engineering Office (Code 504) and prepared by the Computer Sciences Corporation Systems Management Office under the Systems, Engineering, and Analysis Support contract. This document provides a standards baseline for development and maintenance of products developed under the auspices of the Renaissance program for Ground Data Systems.

This document is under the configuration management of the Systems Engineering Office, Code 504.

Configuration Change Requests (CCRs) to this document shall be submitted to the Systems Engineering Office, along with supportive material justifying the proposed change. Changes to this document shall be made by document change notice (DCN) or by complete revision.

Questions and proposed changes concerning this document shall be addressed to:

Gary F. Meyers
Systems Engineering Office, Code 504
Goddard Space Flight Center
Greenbelt, Maryland 20771

Abstract

This document specifies the standards and guidelines for use in constructing Renaissance architecture-based mission systems. This version is aligned with the Renaissance Generic Architecture, Version 2.0. These standards apply directly to Renaissance products, including both software products and delivered systems.

The standards proposed for Renaissance include selections from Federal Information Processing Standards, National Aeronautics and Space Administration, other standards organizations and commercial sources. The primary criteria for inclusion are:

- Value to the Renaissance effort in cost savings, configuration flexibility, or product quality
- High probability of stability over time and missions supported
- Wide applicability and availability
- Support by commercial products and vendors under consideration by Renaissance

Keywords: standards, spacecraft data processing

Contents

1 Introduction

2. Standards Selection

3. Sources for Specifications and Information

Appendix A. IETF RFC Summary

Appendix B. Consolidated Standards Table

Acronyms and Abbreviations

Glossary

Bibliography

List of Figures

List of Tables

1 Introduction

1.1 Purpose

This document defines the standards and guidelines used to support the Renaissance objectives of mission implementation from off the shelf components, using a minimum set of common interfaced, configuration flexibility, and technology evolution. The purpose is to provide a baseline for Renaissance mission system design and building block selection.

1.2 Scope

This document specifies the standards and guidelines for use in constructing Renaissance architecture based mission systems. These standards are applicable for the integration of space mission systems and for the development of those components selected for mission implementation, both MO&DSD products and mission specific components. The standards focus on the systems to be developed rather than the process by which they are developed.

Standards are those specifications that apply directly to Renaissance products, as described in the section defining the standard. They can be *mandatory*, i.e., must always be used, *options*, i.e., a set from which to choose, or *elective*, i.e., selectable when applicable to the situation.

1.3 Approach to Selecting Standards

The approach to selecting standards is to match potential standards to the objectives of Renaissance, and assess the value and cost of applying a candidate standard. Standards serve as enabling technologies for meeting four critical Renaissance objectives. The first objective is to maximize reuse of off-the-shelf components. The second objective is to ensure that the many elements of a Renaissance-based system can be integrated using a minimum set of common interfaces. The third objective is to support a high level of mission configuration flexibility by allowing free interchange of both custom and commercial applications in the configuration of a mission system. The fourth objective is to support development of software elements that address requirements not met by off the shelf components, or improve technology implementations. Given the Renaissance approach to mission implementation, this last objective implies both platform vendor independence and selection of application interfaces appropriate for wide integration.

These standards and guidelines are for use in the implementation, maintenance, and operation of Renaissance-based mission systems. The standards proposed for Renaissance include selections from Federal Information Processing Standards (FIPS), National Aeronautics and Space Administration (NASA), other standards organizations, and commercial sources. The primary criteria for inclusion are:

- Value to the Renaissance effort in cost savings, configuration flexibility, or product quality

- Stability over time and missions supported
- Wide applicability and availability
- Support by commercial products and vendors under consideration by Renaissance

Although the set of standards was chosen on the basis of probable stability, the set varies considerably in maturity. Some are emerging standards, and others are not yet widely implemented in vendor products. These are specified only to point to their future application, and are so described in their respective sections.

It is anticipated that future missions will be developed under new mission implementation procedures that will optimize the business goals of MO&DSD and take advantage of new technology. The standards are organized along process boundaries that were identified by the stability and wide applicability criteria. Those aspects that require a common approach but that are likely to evolve rapidly (e.g., development methods and tools) are expected to be controlled primarily through procedures and not standards. The related elements that are expected to stay constant (e.g., product building block interfaces and images) are intended to be primarily controlled by standards.

This standards document contains the approach to applying standards, as well as the candidate standards specifications. This document includes only high level descriptions and references to standards specifications originating with other organizations. It does not include the complete standards specification. This simplifies inclusion of standards controlled by many organizations, and to minimize the need for change to this document caused by evolving standards definitions.

The Renaissance standards have been separated into global and mission specific categories. The global Renaissance standards are intended to be only those that are to be met by all mission configurations. It is expected that these global Renaissance standards will be supplemented for each mission by mission-specific standards. In some cases, currently held standards are not included as global, because the standards have been deemed to be mission-specific rather than at the Renaissance level. These mission specific standards provide a mission level consistency for areas in which no single standard allowed sufficient flexibility, or in which single standards did not provide any obvious gain in mission capability.

Standards have also been separated into integration and development categories. Integration standards are those which have the primary effect of standardizing interfaces for both COTS and any developed components. Development standards are those which primarily guide the development of mission components, either globally or for a specific mission.

The standards identified in this document are intended to match systems implemented based on the Renaissance Generic Architecture, Version 2.0. Given the current rate of technology change, it is anticipated that the selected standards will change. This document will be updated to reflect changes in technology.

1.4 Document Structure

Section 2 specifies applicable standards, i.e., those standards that a Renaissance mission system implementation is expected to meet. Each subsection addresses a specific objective, the approaches to meeting that objective, and the standards that apply.

Section 3 contains references to standards information, including standards control organizations and reference documents. The source organizations control and provide the detailed documentation of all selected standards. Contact points are included, to support acquisition of the standards specifications.

There are two appendices. Appendix A contains the current (November 1995) set of all standards identified by the Internet Engineering Task Force (IETF), the control organization for all Internet related standards. These are the primary guiding standards for Renaissance. The IETF updates this list on a regular basis, with annual summary documents. All IETF standards are identified as indexed Requests For Comment (RFCs), though not all RFCs are standards. The tables in this appendix are drawn from RFC 1920.

Appendix B contains summary tables of all selected Renaissance standards. These tables are organized by the global, mission specific, integration, and development categories.

2. Standards Selection

This section contains the specification of standards applicable to mission system integration. Each subsection addresses the standards that apply to a specific aspect of the Renaissance architecture. For each aspect, the standards are further organized in a hierarchy of application:

- **Global Mission Integration**: the essential integration standards. These are also the foundation for the other three categories. For the most part, these standards are mandatory.
- **Global Development**: the standards added to the Global Mission Integration standards for the development of MO&DSD multimission products. These standards may be mandatory, optional, or elective.
- **Mission Specific Development**: the standards, added to those of Global Development, that apply to the development of mission unique components. These standards tend to be elective.
- **Mission Specific Integration**: the added standards that are included for use in integration of any specific mission system. The added standards are intended to support integration with mission unique customer, or implementer, systems. It is NOT expected that these added standards will be used for any development, but simply for integration with existing products and other components. These standards tend to be elective.

Given that technology is always advancing, new standards may be added to these lists as necessary. To minimize the risk of adding new standards, the hierarchy will be used to evolve standards. New standards may be experimented with at a mission level. If the standard proves to be useful in a wider range of missions, then the standard will evolve to the global level.

2.1 Network Services

It is important to note that, for many aspects of mission system implementation, detailed knowledge of the network standards is not required. Commercial products exist that perform the required low level activities, e.g., protocol handling, that directly depend on the standards detailed specifications. Only when constructing a custom product that implements a controlled interface and function are the details needed. A general knowledge, and some details, are required when configuring and managing network services, but it is not expected that mission systems will generally be constructing network protocol specific components.

2.1.1 Communications Protocols

The critical integration element for distributed mission systems is the communications mechanism. The entire Renaissance approach to architecture depends on common communications protocols to support ready data transport and interprocess communications. Standardizing communication protocols provides a stable interface for distributed applications

and enables a common set of communication applications to support these protocols and related utility functions. Vendor independence is essential to avoid a very high-cost impact for integration of Renaissance systems and for maintaining hardware vendor independence. At the same time, the intent is to allow enough flexibility to retain the Renaissance approach of using different underlying technologies to meet performance requirements.

The solution is based on the nearly universal Internet Protocol suite defined by the Internet Engineering Task Force. The use of the Internet Protocol (IP) for the network layer is required. Similarly support for all standards for the transport layer, currently the User Datagram Protocol (UDP) and Transmission Control Protocol (TCP), is required. For the higher level protocols and utilities, protocols are to be selected from the accepted IETF standards. For the bottom two layers of the International Standards Organization (ISO) reference model, selection from IETF approved standards would be the norm, with allowance for alternatives for space link protocols. This allows the mission to select low-level implementations, e.g., 10Base-T and Ethernet or Fiber Distributed Data Interface (FDDI), which meet the mission-specific needs for performance and reliability. Further, the standards are supported with products that are both readily available and useful. Note that the term "internet" has a variety of applications. See the Glossary for details.

Additions to this are made for the unique aspects of the space communications in missions, in the form of standards developed under the auspices of the Consultative Committee for Space Data Systems (CCSDS). These standards, combined, form the foundation for the Renaissance architecture.

2.1.1.1 Global Mission Integration Standards

The communications standards categorized as Global Mission Integration provide the essential glue for integrating processes across platforms in a distributed system. They are listed in Table 2-1, and comprise a very short list. All the IETF standards included are to be supported by implemented systems.

Table 2-1. Global Mission Integration Communications Standards

Host Requirements - Communications, RFC1122
Host Requirements - Applications, RFC1123
Internet protocol, RFCs 791, 950, 919, 922
Internet Control Message Protocol, RFC792
Internet Group Multicast Protocol, RFC1112
User Datagram Protocol, RFC 768
Transmission Control Protocol, RFC 793
Routing Information Protocol (RIP), RFC 1058
Profiles for Open Systems Internetworking Technologies (POSIT), FIPS PUB 146-2

Due to the wide usage of the Internet Protocols (TCP-UDP/IP) and their current acceptance within the NIST Profiles for Open Systems Internetworking Technologies (POSIT), IP is

specified as a preferred alternative to Open Systems Interconnect (OSI) and other protocols. As a result, the entire protocol suite is intended for inclusion, including the Internet Protocol (IP), Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and compatible protocols in the other layers of the reference model.

Several extensions to IP and TCP that are relevant to Renaissance have been proposed. IP Multicasting provides a method for transmitting IP datagrams to a group of hosts. The host interface for IP Multicasting (RFC 1112, Internet Group Multicast Protocol) is already standardized and included as part of the IETF Standard Set (STD) 5, Internet Protocol. A new version of IP has been proposed and approved as a proposed standard (IPv6, RFC1752), but has no significant product support at this time. Extensions to TCP have been proposed to provide more efficient operation over networks with latency being dominant over bandwidth, e.g., RFC 1323, TCP Extensions for High Performance. See the required and recommended RFCs in Table A-1 for a complete set as defined in November 1995. Draft standards for future evaluation are included in Tables A-3, A-4 and A-5.

The RIP standard is the only one in general use today. However, it has some serious limitations, and new standards have been developed by the IETF and are being evaluated. These are expected to replace RIP, and are currently listed as Global Development Standards for inclusion in future products.

The revised FIPS POSIT standard modifies FIPS 146-1 by removing the requirement that Federal agencies specify Open Systems Interconnection (OSI) protocols when they acquire networking products and services and communications systems and services. Federal agencies are encouraged to use open voluntary standards when acquiring data communications protocols.

2.1.1.2 Global Development Standards

For global development, there are essentially two types of added standards: anticipated revisions, and network implementation-specific protocol standards, including space-specific standards. These standards are listed in Table 2-2. The anticipated standards included are the proposal for the next generation of IP (IPv6) and the RIP2 and OSPF2 draft standards. These are the only ones that appear as probable future IETF standards. The set of implementation-specific protocols provides the standards for IP compliant implementations of protocols at ISO levels 1 and 2. The implementations include versions for wide and local area networks, and for serial line protocols compatible with standard telephone lines. The space-specific standards are those most essential and most stable for implementation of the RF links between the ground and mission spacecraft. These are equivalent to IETF network specific protocols, but the CCSDS participates in other standards processes, notably ISO, and not in the IETF.

The IPv6 RFC addresses a number of important IP issues: address space, security, optional extension flexibility. It has received serious interest, but may not result in significant implementations for several years. It is fully compatible with existing installations of IP, and supports mixed mode operations. The purpose in including this RFC at this time is to alert application developers to include any implications of this in their designs, to avoid premature obsolescence. Inclusion of this standard is elective by the system developers.

RIP2 and OSPF2 provide updated and improved approaches for routing. Developed systems need to consider the possible implications of compliance for future networking components.

All the RFCs listed for implementation of lower level protocols are existing IETF standards. It is expected that a system will support one or more physical networks and, for each physical network supported, the appropriate protocols from Table 2.2 must be supported. Generally, products will be developed to allow use of any of these standards. However, there are some types of network-related components that may require development associated specifically with one or more of these. An example of a component for which these apply may be a separate gateway for conversion of spacecraft data between space link protocols and terrestrial transport protocols. The intent of not including all such RFCs is to limit product implementation to those in common use. These standards are to be used as electives, in that not all will be used within any given system. However, implementations with protocols not in the list are to be avoided because of the risk of incompatibility.

Table 2-2. Global Development Standards

Recommendation for IP Next Generation (IPv6), RFC 1752
RIP Version 2 - Carrying Additional Information, RFC1723
Open Shortest Path First Routing (OSPF), Version 2, RFC1583
Point to Point Protocol (PPP), RFC 1661
Transmission of IP over Serial Lines, RFC1055
Classical IP and ARP over ATM, RFC1577
Multiprotocol over Frame Relay, RFC1490
Multiprotocol Encapsulation over ATM, RFC 1483
Transmission of IP and ARP over FDDI Net, RFC 1390
Internet Protocol on FDDI Networks, RFC 1188
Address Resolution Protocol, RFC 826
A Reverse Address Resolution Protocol, RFC 903
Internet Protocol on Wideband Network, RFC 907
Internet Protocol on Ethernet Networks, RFC 894
Internet Protocol on Exp. Ethernet Nets, RFC 895
ISO Transport Service on top of the TCP, RFC1006
Packet Telemetry, CCSDS 102.0-B-3
Telecommand Part 1- Channel Service, CCSDS 201.0-B-1
Telecommand Part 2 - Data Routing Service, CCSDS 202.0-B-2

RFC-1006 provides TCP emulation of TP0 for use with OSI applications. The IETF is working towards interoperability with OSI protocols, and this provides for interoperability of valuable applications from the OSI environment.

Space Communications is a unique environment. The requirements for missions supported by NASA frequently have unusual constraints based on the orbits of the spacecraft and on the data requirements associated with operations and payload activity. In particular, the deep space

missions, and those in Lagrange orbits of the sun-earth-lunar sets, have unique problems because of the latency and signal to noise resulting from simple distance. As a result, different technologies have been developed, collected and standardized as the CCSDS standards, which provide a common, packet-oriented approach to space telecommunications.

CCSDS standards have not yet achieved general acceptance, and COTS implementations are scarce. Additionally, the standards, as they exist, make it difficult to completely standardize implementation, making use complex and expensive. Further, it is only very recently that there have been efforts to normalize these communications approaches with the general ones of the earlier section.

The central approach being identified is to convert the CCSDS approach to a layered communications protocol based on the OSI layered model. In this approach, the common Internet protocols would be used for the network and transport layers, at a minimum. The primary approach has much to offer, but is not yet agreed upon. The expectation is that for earth orbiting spacecraft, up to geosynchronous at least, the preferred approach would have CCSDS encoding as a data-link and physical layer protocol, with IP and UDP/TCP layered over this for transport. This would support use of common technology and applications over the network, more effectively integrating the spacecraft into the overall network. Prototypes for this are currently in progress at GSFC and perhaps elsewhere. Other options are being investigated by JPL and DoD. At least one alternative is being studied which provides a transport level interface, but not true internet implementation for network and transport protocols.

Given this status, only those parts of the CCSDS standards that are generally applicable are included in Table 2-2. Implementation using these standards is elective in the sense that they are expected to evolve, and use of replacement standards is to be expected.

Most future NASA space systems are being developed to use CCSDS standards, for a common, packet-oriented approach to space telecommunications. At least one, Landsat-7, is being developed to use the defined CCSDS bitstream mode, limiting standardization. Spacecraft will be expected to conform to this standard, and ground station systems are expected to further support this approach. Most future supported systems will meet at least the minimum requirements of this standard, and the NASA space communications networks will also support the standard. Although currently developed systems adhere to the CCSDS transfer frame standards, not all missions observe the CCSDS standards for other services. Renaissance will encourage adherence to CCSDS standards for all space link services used by a mission by providing common space and ground system components; however, the architecture must allow insertion of mission-specific components to process nonstandard telemetry structures when needed.

Additionally, some legacy missions (e.g., STS and HST) will continue using non-CCSDS methods, and may be required to be supported by new systems in the future. Thus, solutions should be developed which can be modified to support both the hoped for future changes, and legacy spacecraft.

2.1.1.3 Mission Specific Development Standards

For Mission Specific Development, the remaining implementation level CCSDS standards are added. These have been placed here because these standards are incomplete, and usage is evolving. The intent is to use these in the absence of any better approach. If and when better implementations are developed, these standards should be modified to accommodate them. The use of these is considered elective. These standards are listed in Table 2-3.

Table 2-3. Mission Specific Development Communications Standards

Advanced Orbiting Systems (AOS), Networks and Data Links, CCSDS 701.0-B-2
Telecommand Part 2.1 - Command Operation Procedures, CCSDS 202.1-B-1
Telecommand Part 3 - Data Management Service, CCSDS 203.0-B-1

Missions under current development, such as the Earth Observing System and the International Space Station, employ Version 2 virtual channel data units (VCDUs) per the Advanced Orbiting Systems specification. However, existing systems employ the Version 1 transfer frame (VCDU) per the packet telemetry specification. Thus, both standards are listed.

2.1.1.4 Mission Specific Integration Standards

For Mission Specific Integration, additional Internet and CCSDS standards are specified. The added Internet standards are intended for use only where needed, and only when off the shelf components can be purchased to implement them. The CCSDS standards are guidelines for integration and operations. The use of these standards is considered elective. Table 2-4 lists these standards.

Table 2-4. Mission Specific Integration Communication Standards

IP Multicast over Token-Ring LANs, RFC1469
IP and ARP on HIPPI, RFC 1374
X.25 and ISDN in the Packet Mode, RFC1356
Internet Protocol on IEEE 802, RFC1042
Transmission of IP over Serial Lines, RFC 1055
Transmission of 802.2 over IPX Networks, RFC 1132
Telemetry Summary of Concept and Rationale, CCSDS 100.0-G-1
Telecommand Summary of Concept and Service, CCSDS 200.0-G-6

The rationale for including the IETF standards is to indicate the existence of this body of commercially implemented IP standards that may be needed for customer integration in specific network implementations. The CCSDS standards are provided to supply a list that may be useful for some mission integration activities.

2.1.2 System Management

System management is intended here to include management of the system networks, platforms, and processes. The current state of standards is less than ideal. No current standard meets all needs for effective system management (vice network management), and there is little prospect for a consensus in the near future. Because of the absence of true system management standards, the following standards are devoted to network management, for which there is a growing body of available standards and off the shelf compliant hardware and software components.

2.1.2.1 Global Mission Integration Standards

As with communications standards, there are only a few selected as global standards. Simple network management protocol (SNMP) is the base standard, as it has become widely accepted for local area network (LAN) management and is expected to be the core implementation protocol for Renaissance systems in the immediate future. The IETF intends that all IP networks be manageable, and the current definition of that is through the SNMP standards listed in Table 2-5.

Table 2-5. Global Integration Management Standards

Simple Network Management Protocol, RFC 1157
Structure of Management Information, RFC 1155
Concise MIB Definitions, RFC 1212
Management Information Base-II, RFC1213

RFC-1157 provides the definition of the protocol. The other RFCs provide definition of the MIB, which is the data source for exchange of management information between the managed object and the management application. It is acknowledged that SNMP has some significant limitations. Revisions to SNMP are in progress, and some of the leading proposed standards are listed under global development standards for future implementations. The intent is that SNMP should be generally supported on all networks because of the large number of applications and components available that are compliant with the standard.

2.1.2.2 Global Development Standards

The Global Development standards are intended as supplements to the SNMP standards for implementation. They include complementary standards which are currently implemented, as well as the SNMP upgrades mentioned above. The full list is provided in Table 2-6. It is intended that all developed products will be compliant with these. The X/Open standard is preferred because of the flexibility of products developed with this standard. If a product does not use this, then it must be compliant with one of the specific protocols in Table 2-6.

X/Open has developed a standard (XMP) which allows for simultaneous and transparent use of both SNMP and CMIP. There are three specifications available for this, and implementations are expected to be commercially available soon.

Table 2-6. Global Development Management Standards

X/Open Management Protocols API (XMP), X/Open CAE Specification C306, ISBN 1-85912-027-X
X/Open Management Protocols Profile (XMPP), X/Open CAE Specification C206, ISBN 1-85912-018-O
X/Open Managed Objects Guide, X/Open Guide G302 ISBN 1-85912-006-7, 9/93
Common Management Information Protocol (CMIP), ISO9596
Remote Network Monitoring (RMON) MIB, RFC1757
Ethernet MIB, RFC 1643
Government Network Management Profile (GNMP), FIPS PUB 179-1

The common management information protocol (CMIP) is included as a possibility, as it appears to be the direction for commercial wide area network (WAN) management, even though the number of existing products is relatively small. CMIP provides some significant capabilities above that provided by the current SNMP in the areas of security and WAN management.

The RMON standard (RFC1757 in Table 2-6) is included as another option for WAN level system management support. It too has limitations, and is not perceived as a truly long term solution. There are available implementations, however, enabling improved development. SNMPv2 is not currently included, because its form and acceptance are not currently stable. Because of the serious state of management security, and WAN management, there continues to be much activity in a revision to SNMP, but not much fruit right now. All of SNMPv2 is undergoing current revision.

The Ethernet MIB is introduced as a global development standard because of its maturity and pervasive character. While it is appropriate for use in development, it is generally expected that off the shelf components will usually be found for those activities using the standard.

The applicable NIST standard is FIPS PUB 179-1, Government Network Management Profile (GNMP). This FIPS encourages the use of open voluntary standards for the exchange of management information, management functions and services, and the syntax and semantics of the management information required to support monitoring and control of the network and system components and their resources.

2.1.2.3 Mission Specific Development Standards

Mission Specific Development standards, listed in Table 2-7, are added to support mission specific implementations using standards other than the global ones. This may be needed to meet unique mission needs, or to act as a pilot implementation for a standard that is not yet established, e.g., revisions to existing protocols. All of the standards arise from the IETF as either proposed draft standards or experimental standards. Selection for implementation should be based on value to the mission. <u>All are considered elective.</u>

Table 2-7. Mission Specific Development Management Standards

SNMP Distributed Program Interface, RFC1228
MIB Administration of SNMP, RFC1353
SNMP Security Protocols, RFC1352
SNMP Administrative Model, RFC1351
Host Resources MIB, RFC1514
X.500 Directory Monitoring MIB, RFC1567
Mail Monitoring MIB, RFC1566
Modem MIB - using SMIv2, RFC1696
IP Network Control Protocol of PPP MIB, RFC1473
Security Protocols of PPP MIB, RFC1472
Link Control Protocol of PPP MIB, RFC1471
FDDI Management Information Base, RFC1512
FDDI-MIB, RFC1285
ATM Management Version 8.0 using SMIv2, RFC1695
Network Services Monitoring MIB, RFC1565
Source Routing Bridge MIB, RFC1525

The listed SNMP RFCs are proposed standards, addressing some of the critical issues of SNMP. The host resources MIB addresses extension into more of systems management. This is followed by two RFCs for application MIBs that extend the basic IP MIBs. The modem MIB is for modem management, and could be useful for some mission implementations. The remainder are for management of specific network implementations, with extensions to existing standards in some cases, and addressing new categories in others.

2.1.2.4 Mission Specific Integration Standards

The Mission Specific Integration additions are drawn from the IETF Draft Standards and Experimental Standards, and contain RFCs defining MIBs and other aspects of possible SNMP protocols. These standards are provided to indicate where some additional off the shelf applications may be, and what additional standards may apply to customer selected products. SNMPv2 has uncertain status, but some products may exist. When needed, use of products compatible with these is preferable to those with no standards applicable. These standards are electives for mission specific standards selection. The standards are listed in Table 2-8.

One of the serious concerns in Renaissance today is more effective management approaches for spacecraft communications. One group that has the potential to address this problem, and to create standards for such management, is the Mobile Management Task Force (MMTF), a committee from about half a dozen companies. The MMTF has released a set of four draft MIBs, for use within SNMP, which addresses the issues for mobile management. They are proposing these for adoption by the IETF. If this proceeds, these may lead to commercial approaches for integrated communications management for space-based systems.

Table 2-8. Mission Specific Integration Management Standards

IEEE 802.5 Token Ring MIB, RFC 1748
IEEE 802.3 Repeater MIB, RFC 1516
BRIDGE-MIB, RFC 1493
Printer MIB, RFC 1759
MIB SONET/SDH Interface Type, RFC1595
MIB Bridge PPP MIB, RFC1474
Multiprotocol Interconnect on X.25 MIB, RFC1461
SNMP MIB Extension for X.25 Packet Layer, RFC 1382
IP Forwarding Table MIB, RFC1354
Management Information Base for Frame Relay, RFC1315
Frame Relay Service MIB, RFC1604
RDMS MIB - using SMIv2, RFC1697
DNS Resolver MIB Extensions, RFC1612
DNS Server MIB Extensions, RFC1611
Coexistence between SNMPv1 and SNMPv2, RFC1452
Manager-to-Manager MIB, RFC1451
Management Information Base for SNMPv2, RFC1450
Transport Mappings for SNMPv2, RFC1449
Protocol Operations for SNMPv2, RFC1448
Party MIB for SNMPv2, RFC1447
Security Protocols for SNMPv2, RFC1446
Administrative Model for SNMPv2, RFC1445
Conformance Statements for SNMPv2, RFC1444
Textual Conventions for SNMPv2, RFC1443
SMI for SNMPv2, RFC1442
Introduction to SNMPv2, RFC1441

2.1.3 Security

Security is properly a network service, in that system security depends on a system level approach. Acceptance of this need within the Internet community is recent, but activity is now intense. The lack of broadly accepted security standards reflects this historic lack. The most mature protocol standards for security are at the Proposed Draft (Elective) level. Because of need, these are progressing with some current implementations, but no global integration standards are defined for Renaissance.

2.1.3.1 Global Development Standards

Global development standards for security are defined based on two primary sets from the IETF, as shown in Table 2-9. The first set is specified in RFCs 1825 through 1829, which define a security approach for the IP layer. Two IP headers are identified for use: the IP Authentication header, and the IP Encapsulating Security Payload (ESP) header. The second set is defined by

RFCs 1507 through 1510, which prescribe generic security services approach for internet services, supporting and defining both public-key and private-key (or secret-key) cryptography approaches. The public-key approach is founded on the CCITT X.509 standard for infrastructure. X/Open has a security standard based on RFCs 1508 and 1509, and is subsumed under these.

Table 2-9. Global Development Security Standards

ESP DES-CBC Transform, RFC1829
IP Authentication using Keyed MD5, RFC1828
IP Encapsulating Security Payload, RFC1827
IP Authentication Header, RFC1826
Security Architecture for IP, RFC1825
Kerberos Network Authentication Service (V5), RFC1510
Generic Security Service API: C-bindings, RFC1509
Generic Security Service Application Program Interface, RFC1508
Distributed Authentication Security Service, RFC1507
Directory Authentication Framework, CCITT X.509
OSF Distributed Computing Environment (DCE)

The intent is for these global development standards to be used to ensure that components developed for general use do allow for inclusion of these general approaches. These form the basis for much current vendor activity, so non-compliance would have a serious risk of operational incompatibility for any environments using security tools.

The one additional standard in the Global Development domain is the OSF's Distributed Computing Environment (DCE). In the framework for security, the DCE provides an integration of Kerberos authentication with RPCs, directory services and object access that has no viable alternative as a set. DCE is based on international standards, including IETF and ISO products, with a more detailed listing under the network transparency subsection of this document. The intent is that DCE is an option for that class of product aimed at missions needing tightly integrated security. It offers a good environment, widely available even today. In addition to DCE, technology developed by RSA Data Security, Inc. is being incorporated in products by most leading vendors, and RSA is leading an effort for a common firewall approach based on this technology. Developers should be aware of these products and technology.

2.1.3.2 Mission Specific Development Standards

In addition to the above standards, there are a number of current activities that are centered on IETF working group activities. Use of these standards is elective. The Authenticated Firewall Traversal working group has drafts for an authenticated version of the SOCKS protocol that are being taken up by firewall vendors. The Public-key Infrastructure working group is developing a general approach to security based on the X.509 standards. The One Time Password Authentication working group is addressing approaches to negate attacks on internet systems

using passive eavesdropping for passwords. Some implementations based on interim drafts exist, and need to be considered in developing systems. For now, these standards are considered in the domain of Mission Specific Development, and should be considered for this rather than global.

Table 2-10. Security Mission Specific Development Standards

Generic Security Service Application Program Interface, Version 2 (DRAFT)
SOCKS Protocol Version 5 (DRAFT)
Usename/Password Authentication for SOCKS V5 (DRAFT)
GSS-API Authentication Method for SOCKS V5 (DRAFT)
S/WAN Toolkit, RSA Data Security, Inc.
FIPS PUB186 - Digital Signature Standard (DSS), 1994 May 19

In addition to the IETF standards, NIST has published a digital signature authentication standard that is one contestant for this. The NIST standard is FIPS PUB186 - Digital Signature Standard (DSS), 1994 May 19. This standard is added for mission specific integration, as there may be applications available that use this. However most applications appear to be using the technology developed by RSA Data Security, Inc.

2.1.4 Network Transparency

Network transparency consists of a set of network based services that hide the details of the network from the applications. These services rely on platform and communications services for the underlying activity and connectivity. For Renaissance, the model for network transparency consists of:

- Distributed naming services
- Distributed file services
- Interprocess communication services
- Distributed time services
- Distributed user logon services

Standards have been assessed for their effectiveness in providing this functionality, and sorted into the standard categories. In each case, the trade between desirable features of the transparency application and the set of applications that are compatible with it must be made.

Distributed naming services provide a common source to identify network resources. For years, the IETF Domain Name System (DNS) has provided mapping of network host names to internet addresses. More recently, the concept has been extended to include other types of network resources. DCE provides the Cell Directory Service and the X.500 Global Naming Service to allow for network wide location of general network resources, including process groups. Similarly, in the NetWare environment, the NetWare Directory Service (NDS) has been

extended to cover many resource types. Recently, other vendors have been examining the possibility of extending the NDS to non-NetWare environments, but there is not much movement yet.

Distributed file services provide the means for processes to access files across the network. There are two extant types: Transparent File Access (TFA), and file replication. TFA means that files are accessible without direct specification of their network location. It is available in a number of products today, with mixed standards based support. DCE provides the Distributed File System (DFS) which provides for TFA with integrated security. SUN NFS provides equivalent TFA, but with no security extensions. File replication is available most commonly through the IETF File Transport Protocol, which provides the mechanism to copy files between a remote and a local host.

Interprocess communications come in a wide variety of forms. The most common form today is the Berkeley UNIX socket. Variants are common, however, and sockets do not hide much of the network. Better transparency is provided by the Remote Procedure Call (RPC) interface, which cleanly maps to the OSI application level interface, but again variants are common. A completely different approach is taken by the Object Management Group in defining the Common Object Request Broker Architecture (CORBA). The CORBA approach is to provide a broker to link clients to the methods of server objects. The approach is entirely object oriented, but has been used to link in legacy applications through the use of object wrappers.

Distributed time services provide a common time available to all network devices, with the ability to tie into a common time source, and varying levels of precision. The two readily available forms are that provided through the IETF standards, and a related standard service in DCE. DCE claims precision and accuracy to the microsecond level, given the proper time source.

Distributed logon services are also provided in two forms. The more common is that provided by the IETF Telnet, which allows for login to a remote host over the network. More recently, the concept of a single login for the entire network has become of interest. This approach is implemented in the DCE login services, and in several recent non-standardized products.

2.1.4.1 Network Transparency Global Integration Standards

There are only two standards selected as global integration standards. These are listed in Table 2-11 below. Both are IETF standards, and expected to be needed for general use over any internet-based network. The DNS standard provides standard mapping for internet addresses, required for all IP traffic. The file transport protocol is a very basic, and very useful standard supported by any commercial IP product. Neither of these will require development, and both are valuable service standards.

Table 2-11. Network Transparency Global Integration Standards

Domain Name System, RFC1034, RFC1035
File Transfer Protocol (FTP), RFC 959

2.1.4.2 Network Transparency Global Development Standards

The DCE, NFS and CORBA standards have been established as global development standards. These provide very valuable transparency services, but each has limitations. DCE provides the broadest services, but has few applications yet working in the environment. NFS is the most mature, but provides the most limited of services. CORBA is the newest, and addresses key problems for distributed object systems, but is missing critical functions, such as directory services and security, and has only a few COTS products established. The standards are listed in Table 2-12. Along with the DCE, NFS and CORBA standards are those on which these are based (primarily from DCE).

Table 2-12. Network Transparency Global Development Standards

OSF Distributed Computing Environment (DCE)
X/Open DCE: Directory Services, X/Open CAE Specification C312 ISBN 1-85912-078-4, 12/94
ISO/CCITT X.500 Directory Services
Network File System Protocol, RFC1094 (Informational)
NFS Version 3 Protocol Specification, RFC1813 (Informational)
Protocols for X/Open Internetworking: XNFS, Issue 4, X/Open CAE Specification C218 ISBN 1-872630-66-9 (pending IEEE TFA approval)
X/Open DCE: Remote Procedure Call, X/Open CAE Specification C309 ISBN 1-85912-041-5, 8/94
NIST Draft OSF Distributed Computing Environment (DCE) Remote Procedure Call (RPC) Component
OMG CORBA 1.2, Object Management Group's Common Object Request Broker Architecture
OMG CORBA 2.0, Object Management Group's Common Object Request Broker Architecture
X/Open DCE: Time Services, X/Open CAE Specification C310 ISBN 1-85912-067-9, 11/94
Network Time Protocol (Version 2), RFC1119
Telnet Protocol Specification, RFC 854
Related Standards in DCE:
X/Open API to Directory Services (XDS), Issue 2, X/Open CAE Specification C317 ISBN 1-85912-007-5
IEEE Standard for Information Technology 1224.2-1993-Directory Services API-Language Independent Specification (1-55937-302-4)
OSI-Abstract-Data Manipulation API (XOM), Issue 2, X/Open CAE Specification C315 ISBN 1-85912-008-3
IEEE Standard for Information Technology 1224-1993-OSI Abstract Data Manipulation-API [Language Independent] (1-55937-301-6)
X/Open Transport Interface (XTI), Version 2, X/Open CAE Specification C318P ISBN 0-13-353459-6 or C410 (electronic) or C438 ISBN 1-85912-049-0 (Networking services)

The Network File System is a LAN-based application that provides for transparent file access (TFA), i.e., makes remotely hosted file systems transparently available to any application on the client host. It is a client-server product which operates effectively over Local Area Networks. NFS was created by Sun, but has become a very common application in UNIX and PC environments. Note that NFS overlaps with the DCE equivalent (DFS), and should not be used in a DCE environment.

The Distributed Computing Environment (DCE) is a product of the Open Software Foundation, a consortium of computer vendors. DCE provides the basis for most transparency services. DCE services such as remote procedure call (RPC) and distributed time service (DTS) provide significant value-added support in simplifying application development and in meeting performance and data security needs. DCE provides a secure distributed environment by using various services such as Access Control Lists, authenticated RPCs, and Registry Services. The Authentication Service is based on the Kerberos API. The DCE Cell Directory Service and Global Naming Service provide system wide directory services, allowing Client/Server applications to be more flexible. It enables dynamic capability to replicate, backup and move parts of the file system without interruption in service. The Distributed File Service (DFS) is based on the Andrew File System and provides services similar to NFS, but over the entire system, both local and global, and with the Kerberos security woven into the process. Note that Kerberos is referenced in the Security section.

DCE supports both portability and interoperability by hiding differences among varying hardware, software, and networks. For example, DCE RPC automatically converts data from the format of one computer to another. Renaissance will benefit by using these services as part of the network services, but currently the number of applications built to use these services effectively is not large.

The DCE specification is relatively new, but most major UNIX vendors are implementing versions of it. It is also now available in some PC-based environments, providing a wider base for common applications interfaces. This is desirable for Renaissance applications to provide an added API to the operating system file services, and, with the RPC, to assist in standardizing interfaces.

The CORBA architecture is a relatively new technology, but use is spreading rapidly because of the interest in object-oriented designs. The basis of the access architecture has been standardized for some time by the Object Management Group, a consortium of vendors. Products supporting the Common Object Request Broker Architecture (CORBA) are in use, notably Digital Equipment Corporation's (DEC's) Application Control Architecture product and Iona's Orbix product. The current problem is that the differing products, primarily based on CORBA 1.2, do not work together.

This problem has been resolved with the follow-on standard (CORBA 2.0) released in December 1994. Some products, such as Hewlett-Packard's Distributed Smalltalk 5.0, are beginning to appear. Other products, such as Iona Orbix, have plans to migrate to CORBA 2.0. Alternative approaches do exist, particularly the object linking and embedding (OLE) specification from Microsoft, but CORBA appears to better meet Renaissance needs. Future development should

consider CORBA as a serious server alternative, even for legacy systems, as it provides access to extended object typing and to a full set of client platforms and applications.

These standards are considered an option set for global product development. For products intended for use in environments requiring significant security, the DCE base is the only one that includes integrated security. DCE's advanced directory services also provide a feature for enhancing system flexibility and reliability through dynamic process mapping. For products requiring only TFA support, NFS is a very stable product available across all platforms being considered. For products based on object oriented implementation, CORBA is the only really useful standard present for distributed objects. At least one version, Digital Object Broker, is compatible with the DCE environment, for the addition of security and directory services. All global development should map into one or more of these standards. Not every component is sensitive to the standards, but should be compliant with the relevant interfaces and restrictions.

2.1.4.3 Network Transparency Mission Specific Development Standards

The mission specific development standards are few, and listed in Table 2-13. They are based on specifications that have not yet achieved the status of standards. Each of these addresses specific problems that may arise, and each is supported by at least some commercial products. The FTP specification provides mechanisms for exchanging very large datasets, such as an extended archive. The ONC RPC specification is a proposed standard incorporating SUN's RPC interface. Finally, the Telnet specification provides a mechanism to integrate Telnet with the user authentication of Kerberos to provide a security plug for remote logins. Each should be noted, and used when appropriate for mission specific purposes.

Table 2-13. Network Transparency Mission Specific Development Standards

FTP Operation Over Big Address Records, RFC 1639
Binding Protocols for ONC RPC Version 2, RFC1833
Telnet Authentication: Kerberos V4, RFC 1411

2.1.4.4 Network Transparency Mission Specific Integration Standards

Only one additional specification is currently identified for mission specific integration, as shown in Table 2-14. The Novell NetWare environment is a very common one in enterprise networks, and is likely to be encountered in customer integration. Additionally, there is a potential for the NDS to become a more widely available product, i.e., in the internet environment. In that case the status of this would be upgraded as directory services are a very valuable addition to network services. Use of this standard is elective and is based on the existing or planned presence of NetWare in the customer environment.

Table 2-14. Network Transparency Mission Specific Integration Standards

NetWare Directory Services (NetWare 4.1), Novell

2.2. Network Applications

The following sections describe application standards that apply to network services. Most are derived from IETF standards, but the network transparency applications are outside this environment, having been developed by outside vendor consortia.

2.2.1. Electronic Mail

The standards based protocols for E-mail in use are X.400 and the Simple Mail Transfer Protocol (SMTP). GSFC has mandated that SMTP/MIME be used by all GSFC systems. If MO&DSD is to market to other customers, there is some possibility that X.400 may need to be considered on a mission specific basis for reasons of customer compatibility.

2.2.1.1 Global Integration Standards

SMTP is the E-mail protocol used for UNIX and the Internet Protocols. It has wide acceptance with over 30 million users and growing. SMTP provides Internet access, and is supported on UNIX, PC and Macintosh platforms. It is a low cost solution with wide availability of public domain products. Multipurpose Internet Mail Extensions (MIME), which was added to SMTP, enhances the existing capabilities of SMTP. Some of these capabilities are as follows:

- Unlimited line length
- Use of multiple objects in a single message
- Use of characters sets other than ASCII
- Use of multiple fonts in a message
- Binary files
- Multimedia message environment

MIME allows messages to be of any length. It is compatible with older versions of SMTP and has recently become usable from windows based applications. It has benefits to Renaissance in that it conforms to open standards. One of its best features is that allows simple addressing formats. An advantage over X.400 is that, if you choose to use a different carrier to access the Internet, you don't have to change your E-mail address, while with X.400 you have to make the necessary changes. SMTP/MIME supports all data types Renaissance is likely to use for the near future. The standards for SMTP and MIME are listed in Table 2-15.

These global integration standards should be supported by all systems developed. For Email, this means that SMTP mail should be used, for general integration purposes. Even in the event of a specific mission, in which the entire system is dedicated to a customer site, use of a customer selected Email system other than SMTP-based is discouraged, because Email-enabled applications will not be generally compatible with such a system.

Table 2-15. Electronic Mail Global Integration Standards

Simple Mail Transfer Protocol, RFC821
SMTP Service Ext for Message Size, RFC1870
SMTP Service Extensions, RFC1869
Multipurpose Internet Mail Extensions (MIME), RFC1521
Format of Electronic Mail Messages, RFC822
Content Tupe Header Field, RFC1049

2.2.1.2 Global Development Standards

There are open issues pertaining to the SMTP standard. The primary concerns are those risks at the center of the operational systems: integration with automated processes, security, and data reliability. Some of these issues are the focus of current IETF activity. In particular, security standards are rapidly maturing, and can be added to the list of Global Development standards. The recent addition of Privacy Enhanced Mail (PEM) standards solves some of the major security issues by adding user controlled encryption. These standards, listed in Table 2-16, cover the four basic security issues of authentication, privacy, data integrity, and non-refutability. They are developed around the security standards listed in section 2.1.3.

Table 2-16. Electronic Mail Global Development Standards

PEM - Key Certification, RFC1424
PEM - Algorithms, Modes, and Identifiers, RFC1423
PEM - Certificate-Based Key Management, RFC1422
PEM - Message Encryption and Authentication, RFC1421
MIME Object Security Services, RFC1848
MIME: Signed and Encrypted, RFC1847

These standards are to be used whenever products are developed, so that mail-enabled applications are compatible with the security requirements, and can be operated with such mail systems.

2.2.1.3 Mission Specific Development Standards

Additionally, there are a number of experimental extensions that may be of interest in the future, extending the ability of MIME to handle multimedia and other large attached files. These standards are added under Mission Specific Development, as options for consideration for a specific mission implementation, and are listed in Table 2-17.

Table 2-17. Electronic Mail Mission Specific Development Standards

SMTP 521 Reply Code, RFC1846

SMTP Service Extensions for Checkpoint/Restart, RFC1845
SMTP Service Ext. Large and Binary MIME Msgs., RFC1830

2.2.1.4 Mission Specific Integration Standards

An additional consideration for mission specific integration is the possible presence of X.400-based systems in customer sites. A number of these exist for large organization support, using standard commercial tools. While gateways exist to X.400, conversions between the two may need to be considered when integrating. Relevant standards for the interfaces and interchanges are shown in Table 2-18.

Table 2-18. Electronic Mail Mission Specific Integration Standards

MIME encapsulation of EDI Objects, RFC 1767
MIME encapsulation of Macintosh files, RFC 1740
X.400/MIME Body Equivalences, RFC1494
MHS/RFC-822 Message Body Mapping, RFC1495
Mapping Between X.400 (1988), RFC 1327
X.400 Use of Extended Character Sets, RFC 1502
Postmaster Convention X.400 Operations, RFC 1648

In addition, the major commercial Email products, e.g., Lotus cc:Mail and Microsoft Mail, are likely to be found in customer or third party development sites, and gateways to these will be needed. As these are product specific, they are not called out as standards.

2.2.2. World Wide Web

Interchange of documentation, both static and active, across mission systems is important for operations and as a form of product delivery mechanism. A standards based solution to this is the family of applications called the World Wide Web. The heart of the solution is a client-server approach, with both a server and a networked browser client. The common interface employs Hypertext Markup Language (HTML), which is a Standard Generalized Markup Language (SGML) document type, and the Hypertext Transfer Protocol (HTTP). The virtue of this approach is that the browser provides the entire environment for interacting with the server in a standard way, independent of the host platform, and of location on the network.

The Web is rapidly becoming a promising area for commercial development. Recent developments include new drafts of HTML, and the creation of an environment for distributed object applications (HotJava) by Sun, that is rapidly being adopted as a de facto standard. Available products are rapidly outstripping the standards process, with the attendant risk that vendor unique implementations will not be widely supported. The IETF is providing a mechanism for rapid change management through the RFC process.

2.2.2.1 Global Integration Standards

Those standards that are well established are set as global integration standards, as shown in Table 2-19. They are needed at the integration level to ensure the universal support of the general Web capabilities, as currently implemented.

Table 2-19. Global Integration Standards

Hypertext Markup Language - 2.0, RFC 1866
Form-based File Upload in HTML, RFC 1867
Relative Uniform Resource Locators, RFC1808
Standard Generalized Markup Language (SGML), FIPS PUB 152

The first three standards comprise the basic current definitions of Web products. Any products developed for use in the Web must comply with these. SGML is the parent standard for HTML, i.e., HTML is a subset of SGML.

2.2.2.2 Global Development Standards

Two additional standards are added as global development standards. These two draft standards are the current working versions of the security approaches for use with the Web. These are not final, and there are competing, non-standardized approaches being explored. For Web products being developed, the implications of the security issues and approaches should be addressed using these standards at a minimum. These should be applied only in product environments requiring trusted Web service. They require integration with the general security services described in section 2.1.3. The standards are shown in Table 2-20.

Table 2-20. Web Global Development Standards

The Secure HyperText Transfer Protocol (DRAFT)
Use of the GSS-API for Web Security (DRAFT)

2.2.2.3 Mission Specific Development Standards

There are no standards, per se, at the mission specific development level. However, the Java environment is rapidly becoming a de facto standard. For now, this is considered at this standards level, since a mission system may be an appropriate approach for a pilot for Java applications. Note that it is the run-time environment that is specified here. Java language specification is discussed in the development section.

2.2.2.4 Mission Specific Integration Standards

As with mission specific development standards, there are no true standards declared at this level. It is intended that use of product specific approaches be allowed at this level. Examples of this would include use of specific vendor servers, e.g., Netscape servers, with useful features such as security or Java run time environment support. When use of such products allows the avoidance of development, then alternative implementations are the preferred approach.

2.3 Data Management

The purpose of the data management standards is to provide a common method for storing, retrieving, and managing datasets. The Renaissance standards for data management apply to the logical schema of the data, not to the physical schema. In this way, missions can choose from a number of products that meet the standards. For the most part, data management standards apply to the selection and integration of database management systems. Some DBMS applications also allow for the integration of flat files (either through import mechanisms into the database or middleware interfaces to the files).

2.3.1 Global Mission Integration Standards

The data management standards for global mission integration are listed in Table 2-21.

Table 2-21. Global Mission Integration Data Management Standards

Database Languages -- SQL, ISO/IEC 9075:1992
Database Language SQL, ANSI X3.135-1992
Database Languages - SQL - Part 3: SQL Call Level Interface (SQL/CLI), ISO/IEC DIS 9075-3
The Object Database Management Standard: ODMG-93 , ed. by R. Cattell, Morgan Kaufmann Publishers, 1994

The Structured Query Language (SQL) is the international standard for database update and retrieval. This standard is accepted for global mission integration for Renaissance missions, due to the large number of existing COTS products that adhere to the standard. The standard covers the following areas of data management:

- Schema definition, to declare the structures, integrity constraints, and access privileges of a database,
- Schema manipulation, to alter a schema definition,
- Data manipulation, to populate a database and access SQL-data,
- Transaction management, to define and manage SQL-transactions,
- Connection management, to establish and manage SQL-connections,
- Session management, to set the attributes of an SQL-session,

- Dynamic SQL, to provide facilities for dynamic construction and execution of SQL statements,
- Diagnostics management, to communicate constraint violations and warnings to applications,
- Information schema tables, to provide an SQL description of schema definitions,
- Programming language bindings, to declare database procedures that may be called from various programming languages,
- Embedded SQL, to define how SQL statements may be syntactically embedded into one of the following programming languages: Ada, C, COBOL, FORTRAN, MUMPS, Pascal, or PL/I.

In addition to the current SQL standard, ANSI and ISO have published a draft call level interface (CLI) standard based on Microsoft's Open Database Connectivity (ODBC) interfaces. Products that conform to this standard can interact through database calls. Since a large number of applications and database management products already conform to the ODBC interfaces, this draft standard has been added to the Renaissance data management standards.

In addition to the SQL standards, standards have been included to cover object-oriented database management systems (OODBMS). As object-oriented products become more prevalent, there will be a need to store persistent objects. These standards are not as mature as the SQL92 standards. Two areas show promise as standards for OODBMS's: The Object Data Management Group's ODMG-93 and extensions to the SQL standard.

ODMG-93 is an extension of the work done by OMG. The object model is based on the OMG object model. ODMG-93 is intended to allow portability of applications across OODBMS products and has included an object definition language standard based on the OMG CORBA IDL and an object query language (OQL) as an extension of SQL. The intention is that any application written to the ODMG-93 standard will work with any OODBMS that meets the standard with a recompile (currently ODMG-93 defines bindings to C++ and to Smalltalk). Since ODMG has no mechanism for documenting standards, the standard is published as a reference book. The current standard is version 1.2, which was released in December 1995.

Modifications to the SQL standard (known as SQL3) are being made by ANSI (X3H2) and ISO (ISO/IEC JTC1/SC21/WG3) to include abstract data types. The current draft specification deals with user-defined abstract data types, including methods, object identifiers, subtypes and inheritance, polymorphism, and integration with external languages. The committee draft is due for release in January 1996 and the international standard is scheduled for release in Summer 1998.

Currently, ODMG-93 shows the most promise for the short term. All members of the ODMG currently ship an OODBMS, and are required to commit to producing an ODMG-compliant product. There has also been some cooperation between the two standards bodies to accommodate the features of each standard.

All of the data management standards are considered elective. The purpose of including these standards is to encourage the use of commercial products that comply to one or more of the standards, so that applications products are not vendor dependent.

2.3.2 Global Development Standards

The global development standards for data management are the same as those for global integration with the addition of the flat file specifications listed in Table 2-22. These standards form an option set for Data Management. The choice of standard to be used in this area is driven by the task that is to be performed and the nature of any existing interfaces.

Table 2-22. Global Development Data Management Standards

FIPS PUB 151-2, Portable Operating System Interface (POSIX) - System Applications Program Interface [with C language bindings] (ISO/IEC 9945-1:1990, POSIX.1)
Microsoft Corporation Windows NT Systems Developer Kit (SDK)

SQL or ODMG-93 should be used for the development of applications with the following additional criteria. Relational database management standards (SQL) should be used for those applications that are table oriented. Storage and processing of telemetry packets is a good example of a relational application. Object-oriented database standards (ODMG-93, SQL3) should be used for applications that manage and manipulate data as objects. For example, storage and processing of telemetry files would use an object-oriented approach.

POSIX.1 defines the file access specifications for the UNIX environment. The original standard has been enhanced with language bindings for Ada and Fortran. The WIN32 API, as defined in the NT SDK, defines the file access specifications for the Windows NT environment. Applications should be written in such a way that they can make use of either interface. For more information applying these standards to development, see Section 2.5.

2.3.3 Mission Specific Development Standards

For data management, the mission specific development standards include all of the earlier standards. In addition, two products that have been chosen for use in this area are shown in Table 2-23.

Table 2-23. Mission Specific Development Data Management Standards

Information Builders, Inc., Enterprise Data Access/SQL (EDA/SQL)
Sybase OmniSQL

The use of these two products is elective because they are single-vendor interfaces. The use of these products depends on the support of the vendor. Also, new products that enter the market

may be added at a later time. These products were not chosen for global development because they are dependent on a single vendor and may change at the whim of that vendor.

2.3.4 Mission Specific Integration Standards

The mission specific integration standards for data management are based on a middleware approach. Any of the standards in the earlier sections may be used, as well as vendor-specific products. For example, if the Oracle Database Management System is chosen for a specific mission, then mission specific integration can be performed using the Oracle interfaces.

2.4. Data Interchange

Data interchange standards were selected because data generated by one application should be available to other applications without extensive conversion or modification to application code. There are two types of data interchange standards: file format standards and data item standards.

2.4.1 Global Integration

Data interchange standards are primarily driven by the availability of software that supports the standards as well as the acceptance of the standard in the user community. Table 2-24 lists the global integration data interchange standards. These standards are an option set, with at least one of he standards to be used.

Table 2-24. Global Integration Data Interchange Standards

ISO/IEC 10918:1994, Information Technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines
CompuServe Inc., Graphics Interchange Format (GIF), Version 89a
ISO/IEC 11172-1:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 1: Systems
ISO/IEC 11172-2:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 2: Video
ISO/IEC 11172-3:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 3: Audio
ISO/IEC 11172-4:1995 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 4: Conformance testing
ISO/IEC DTR 11172-5 Information technology -- Coding of moving pictures and associated audio for digital storage media up to about 1.5 Mbit/s -- Part 5: Software simulation
National Space Sciences Data Center (NSSDC) Common Data Format (CDF)
National Center for Supercomputing Applications (NCSA) Hierarchical Data Format (HDF)
National Center for Atmospheric Research Network Common Data Format (netCDF)
FIPS/PUB 128, Computer Graphics Metafile (CGM)
International Astronomical Union Flexible Image Transfer Standard (FITS)
World Meteorological Organization publication No. 306, Manual on Codes, Vol. 1, Part B, Secretariat of the WMO, Geneva, Switzerland, 1988, plus Supplements

ISO/IEC 10198 describes the Joint Photographic Experts Group format (JPEG). JPEG and GIF are widely accepted standards for the interchange of static visual data (images, etc.). ISO/IEC 11172 defines the Moving Picture Experts Group (MPEG) standard. MPEG is a widely accepted standard for video interchange. Browsers for these formats are available as freeware, shareware, and commercial products for virtually all desktop computers. These formats should be used for any visual data that is to be produced so that it can be easily viewed with any standard viewer.

Several standard file formats are in use in the earth and space sciences communities that have traditionally been served by MO&DSD. CDF, HDF, and netCDF are de facto standards within the earth sciences community for the storage of multi-dimensional data. The standards all share a common heritage. Support for these standards has been demonstrated by the availability of software from the developing organizations and from several user organizations. Also, netCDF and HDF have been incorporated in several commercial visualization packages. The most recent version of HDF includes the netCDF interfaces. FITS is the world-wide astronomical community's standard for the exchange of data. The ability to read and write data files in FITS format has been incorporated into almost every astronomical data analysis package in common use. While all of these formats can be used to integrate science processing systems into the control center, the translation of telemetry data to these file formats will require some development, often in the mission-unique environment.

The World Meteorological Organization is a specialized agency of the United Nations, that is responsible for international cooperation in weather forecasting. For the interchange of meteorological, the WMO has developed the Gridded Binary (GRIB) format for the exchange of grid-oriented data. The US National Weather Service has adopted GRIB as a format for the output of meteorological data. This standard will be applied to any mission systems that need to receive meteorological data (e.g., for use in planning) or that put out meteorological data.

Some seemingly global formats should be avoided, such as the Windows Metafile (WMF) and Bitmap (BMP) formats, since they tend not to be supported across platform domains and are specific to one vendor.

2.4.2 Global Development

The issues driving global development standards for data interchange are product line consistency and customer interfaces. Most of the customer interfaces are included in the global integration standards: CDF, HDF, netCDF, FITS, and GRIB. CDF, HDF, and FITS are to be used for all software products. Software products developed for the creation of scientific products should be able to write outputs in at least CDF, HDF, and FITS. The software products should also be able to read at least one of these formats. Software products developed for use in reading or creating meteorological data products should be able to read and write data in GRIB. The additional global development data interchange standards are shown in Table 2-25.

Table 2-25. Global Development Data Item Interchange Standards

ANSI/IEEE Std 754-1985, IEEE Standard for Binary Floating-Point Arithmetic
ANSI X3.4-1986 (R1992), Coded Character Set 7-Bit American National Standard Code for

Information Interchange

ISO/IEC 646:1991, Information Technology -- ISO 7-bit coded character set for information interchange

The Unicode Standard, Worldwide Character Encoding, Version 1.0, Volume 1, Addison-Wesley, 1990.

The Unicode Standard, Worldwide Character Encoding, Version 1.0, Volume 2, Addison-Wesley, 1992.

ISO/IEC 10646 -1:1993, Information technology -- Universal Multiple-Octet Coded Character Set

Database Languages -- SQL, ISO/IEC 9075:1992

Database Language SQL, ANSI X3.135-1992

Database Languages - SQL - Part 3: SQL Call Level Interface (SQL/CLI), ISO/IEC DIS 9075-3

The Object Database Management Standard: ODMG-93 , ed. by R. Cattell, Morgan Kaufmann Publishers, 1994

CCSDS 620.0-B-2 Blue Book, Issue 2, Standard Formatted Data Units-- Structure and Construction Rules, May 1992

CCSDS 630.0-B-1 Blue Book, Issue 1, Standard Formatted Data Units - Control Authority Procedures, June 1993

CCSDS 641.0-B-1 Blue Book, Parameter Value Language Specification (CCSDS 00006(, May 1992

CCSDS 643.0-B-1 Blue Book, ASCII Encoded English (CCSDS 0002), November 1992

IEEE floating point standard is to be applied whenever floating point data is to be exchanged and no other mechanism is available. It should not be applied if it requires conversion between the applications. ASCII defines the standard for 7-bit text data (although the character set is not complete). Unicode along with ISO/IEC 10646 defines the standard for 16-bit character sets. These standards include the same characters as ASCII as well as several non-Latin alphabets and symbol sets. The Unicode standard should only be used when internationalization is required. Bit order was not considered for standardization. This is a network transparency issue (see Section 2.1.4).

The use of database management systems as a development standard for data interchange is elective. If DBMS's are used, then they must conform to either the relational database SQL standards (particularly the SQL/CLI standard) or the object-oriented ODMG-93 standards. As the object-oriented standards become more prevalent and gain vendor acceptance, it may be appropriate to standardize on OODBMS as the means of dataset interchange.

The CCSDS Standard Formatted Data Unit (SFDU) standards define a structure for the exchange of data between archival sites. These standards have been in use for data interchange between MO&DSD and its customers, including the National Space Sciences Data Center (NSSDC). General data products for dissemination to customers will adhere to these standards. File standards, such as HDF and FITS, will be wrapped within the SFDU structure. Since there are no commercial products that support this standard, it is considered a development standard. The MO&DSD product line should include the ability to generate SFDUs for all data products.

2.4.3 Mission Specific Development

Mission specific development standards are driven primarily by the products that are used by the mission and by the needs of the end-user community. The global integration and development standards apply to mission specific development. Mission specific software will only need to create those formats being used specifically for that mission, and not all of the ones required for global development. In addition to the global development standards, file formats specified by a vendor for interface to their products and formats specified by a customer application may be used. Published APIs should be used to reduce interface problems.

2.5. Platform Portability

Platform portability requires standards that allow the integrator to select and/or develop applications without regard to the platform to be used. In the current environment, there are two hardware vendor-neutral operating systems that allow for this kind of portability: UNIX based on X/Open's Single UNIX Specification and POSIX, and Microsoft Windows NT.

2.5.1 Global Integration Standards

Integration standards for platform portability were selected with the idea that applications should not be tied to a specific platform vendor. To allow for cost flexibility, two sets of operating system standards were selected. These standards are listed in Table 2-26.

Table 2-26. Global Integration Platform Portability Standards

X/Open Publication Set T907, Single UNIX Specification, 1995
Draft Standard for Information Technology, X Window System Graphical User Interface - Part 1: Modular Toolkit Environment, IEEE Working Group P1295.1
FIPS PUB 158-1, User Interface Component of Applications Portability Profile (MIT X Window System)
OSF Motif, Opens System Foundation, Motif Graphical User Interface
X/Open Publication Set T408, XCDE Definitions, Infrastructure, Services and Applications Set
FIPS PUB 151-2, Portable Operating System Interface (POSIX) - System Application Program Interface [with C language bindings], (also published as ISO/IEC 9945-1:1990, POSIX.1)
FIPS PUB 189, Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities, (also published as ISO/IEC 9945-2:1990, POSIX.2)
IEEE 1003.1b-1993, Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension [C Language]
IEEE Working Group P1003.6, POSIX - Security Extensions, IEEE 1003.1e and IEEE 1003.2c
Microsoft Windows NT System Developer's Kit (SDK)

The X/Open Single UNIX Specification defines the specifications that an operating system must meet to be branded by X/Open as UNIX. X/Open owns the trademark to UNIX. Currently, few of the UNIX vendors have complied fully with this specification. However, preference should

be given to vendors that have complied with at least a portion of the specification and which are showing progress toward full compliance.

X11 and OSF/Motif are the UNIX industry standards for user interfaces. X/Open has also defined the Common Desktop Environment, based on an effort by the major UNIX vendors to define a common windowing environment to which all vendors can write software. CDE sits on top of OSF/Motif and provides interoperability across applications.

The POSIX standard complements the Single UNIX Specification by defining a set of portable operating system interfaces. Both standards seek a worthy goal: source code portability across multiple operating systems. This similarity of purpose has resulted in considerable overlap. Operating systems and applications can be compliant with both. They are not mutually exclusive. Since the Single UNIX Specification requires compliance with POSIX.1 and POSIX.2, Renaissance standards require compliance with the Single UNIX Specification for all areas covered, and with POSIX for all other areas. Figure 2-1 shows the overlap between POSIX and the Single UNIX Specification.

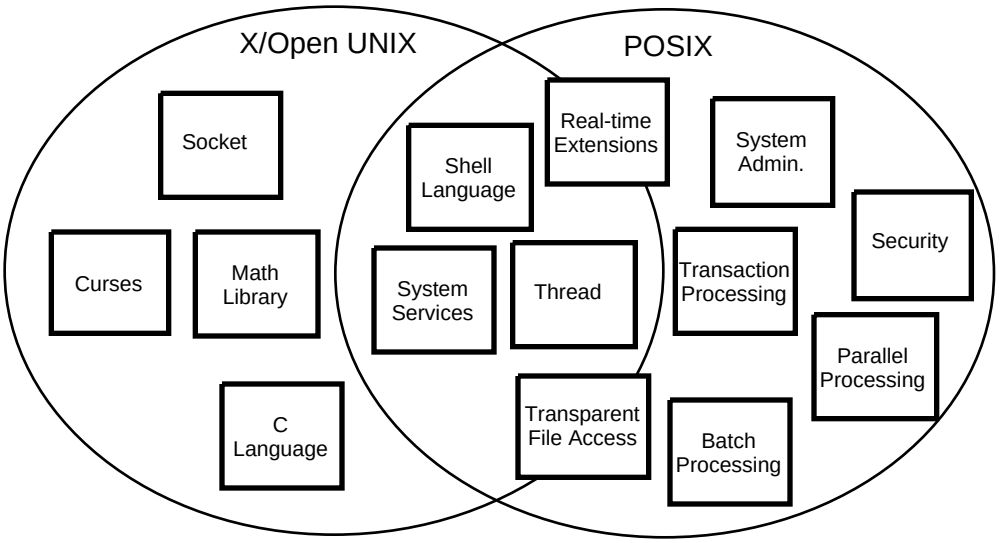

Figure 2-1. X/Open Single UNIX Specification and POSIX Overlap

Compliance testing with these standards is provided through X/Open and the National Institute of Standards and Technology (NIST). X/Open sponsors a branding program that includes the Single UNIX Specification, X11 and OSF/Motif, and CDE. NIST sponsors the compliance program for POSIX.1.

As a lower cost alternative to the UNIX environment, Microsoft Windows NT is also part of the standards. Windows NT was selected since it allows the selection of tools and applications from the Windows 95 environment. These tools can generally be purchased for a fraction of what they cost for the UNIX environment. The use of Windows NT should be tempered with the knowledge that it is a completely proprietary environment. The specifications have been

difficult to find and could change with each release. One advantage to the Windows NT is that Microsoft sponsors Designed for Windows 95 and Designed for Backoffice qualification programs. Both of these programs require compliance with the Windows NT environment. Independent software vendors can submit their software to an independent testing firm and have it tested for compliance at a modest fee.

2.5.2 Global Development Standards

The same standards that apply to global integration standards apply to global development standards as well and should be applied as follows. All applications should be designed and developed to run in both the UNIX environment and the Windows NT environment. The development environment should support development of applications that are platform independent. The applications that are developed should meet the standards to qualify for X/Open branding and the "Designed for Windows 95" logo.

2.5.3 Mission Development Standards

The mission development standards are the same as the global development standards, except it is not anticipated that applications will need to be written for more than one environment. It is also not expected that any mission specific applications will be submitted for the X/Open brand or the "Designed for Windows 95" logo. Only in very unusual situations should mission development be performed for any platform other than UNIX or Windows NT (although applications written for Windows NT should also run on Windows 95).

2.5.4 Mission Integration Standards

The mission integration standards are the same as the global integration standards, with the addition of the Apple Macintosh and the Microsoft Windows 95 environments. These platforms can be fully integrated as clients into the mission system with minimal difficulty. Other systems may be integrated as end-user systems where the customer has a need to transfer data to special applications running on non-standard platforms (for example, science data needing to be transferred to a large model running on a Cray platform). These non-standard platforms would be loosely integrated using well-defined network service interfaces.

2.6 Development Environment Standards

Software development within MO&DSD is changing significantly in nature. In the past, software development included development of the entire system, with little or no OTS software used. In the future, software development will be performed to support the integration of OTS packages or to create selected new products. The purpose of software development will be to create reusable components that can be easily integrated into the mission system or to develop software that can be used in support of OTS integration (e.g., glueware). These components may be programs, functions, or objects. The intention of the development standards is to provide an environment that promotes the development of reusable software and encourages the reuse of already developed software. The development environment standards are divided into four categories: Languages, Tools, Repositories, and Process.

2.6.1 Languages

2.6.1.1 Global Product Development

To promote the development of reusable components, only object-oriented languages may be used may be used for new product development (see restrictions on the use of C and Fortran). The languages currently allowed for product line development are listed in Table 2-27. The use of one of these languages is required for product line development.

Smalltalk was developed at Xerox Palo Alto Research Center (PARC) in the early 1970's. With the recent increased interest in object-oriented programming, use of Smalltalk has increased. Smalltalk is considered a better language than C++ for object-oriented development because it was developed as an object-oriented language, while C++ was developed as an object-oriented version of C. A sign of the increased interest in Smalltalk is that an ANSI committee (X3J20) is working on a Smalltalk standard, with the hope that a draft may be available in 1996. Currently, the best definition of the language is in the publications of the team that developed it. Smalltalk has had a great influence over the development of other object-oriented languages. Almost all of the object-oriented concepts can be traced back to the Smalltalk language. It has also influenced the development of the Macintosh, Microsoft Windows, and OSF/Motif user interfaces.

Table 2-27. Global Product Development Language Standards

Goldberg, A. And Robson, D. Smalltalk-80: The Language. Reading, MA: Addison-Wesley, 1989.
Goldberg, A. Smalltalk-80: The Interactive Programming Environment. Reading, MA: Addison-Wesley, 1984.
ANSI X3J16/95-0088 and ISO WG21/N0688, April 1995 C++ Working Draft. Base documents are Stroustrup, B., The C++ Programming Language (Second Edition) (The Annotated Reference Manual), Addison-Wesley, 1991 and ISO/IEC 9899:1990, C Standard.
FIPS PUB 119-1, Ada (ANSI/ISO/IEC 8652:1995)
FIPS PUB 160, C (ANSI/ISO 9899:1992)
FIPS PUB 69-1, Fortran (ANSI/X3.9-1978, ISO 1539:1980)

C++ is by far the most widely used object-oriented language. C++ was developed at AT&T and an effort has been underway for a number of years to develop a standard for C++. The Annotated Reference Manual by Stroustrup is the currently accepted standard and is evolving to an international standard. Unlike Smalltalk, C++ was developed from another language, C, and carries many of the same features of C. C++ is relatively easy to learn for most C programmers, because of the similarity to the C language. However, there is also a tendency to write C++ programs like C programs and therefore not take advantage of the object-oriented features.

Ada was developed by the US Department of Defense in the late 1970's and early 1980's as the universal language for DoD software. The early versions of Ada were object-based, but not truly object-oriented. Ada 95 is the first version of the popular Ada programming language to be truly object-oriented. The advantage of Ada is that no subsets or supersets of the language are

allowed. Therefore it is possible to develop code on one platform and transport it directly to another platform without source modification.

FORTRAN and C have been the languages used in most of the MO&DSD legacy code. As appropriate, this software may be reused and modified. The ANSI C language [Reference 7] is also acceptable for new code development, but only as an output product of a tool (see Section 2.6.2). No product line code is to be manually written in C and no new development may be done in Fortran.

2.6.1.1 Integration Development Languages

In addition to the languages used for product line development, any of the languages listed in Table 2-28 may be used to develop software in support of mission specific integration (e.g., bridges, translators, glueware).

Table 2-28. Mission Specific Development Language Standards

Sun Microsystems, The Java Programmer's Guide
Aho, A., Kernighan, B. , Weinberger, P., The AWK Programming Language. Addison-Wesley, 1988, ISBN-0-201-07981-X.
Practical Extraction and Report Language (perl), Larry Walls, Documents freely available via many sites on WWW and Internet.
Operating system specific shell languages (e.g., UNIX C Shell)

Java is a new object-oriented language developed by Sun Microsystems, Inc. Java was designed specifically for developing applications for downloading and use in conjunction with WWW browsers. The language is derived from the C++ language with some of the more dangerous features inherited from C removed (such as the use of pointers) and some new features added (such as security). Java is to be used for the development of applets that can be downloaded from web pages. The advantage of the Java language is that it is completely self-contained. Java code is “compiled” into a machine-independent code that is executed by an executive that is built into the Web browser. The Java language is proprietary to Sun. Because Java is a new language, it was not selected as a global standard. Instead, it may be used as a mission development standard to gain experience. If a mission is selected as a trial for using the WWW for mission integration, then Java should be used as the language for developing applets for that mission. Eventually, Java may become a global development language.

Awk is a powerful text manipulation language developed by Aho, Weinberger, and Kernighan (hence awk), at AT&T. The language is generally available on any UNIX platform and versions have been developed for Microsoft platforms as well, including a gnu version from the Free Software Foundation called gawk. Awk can be used as a file format translator to bridge output from one application to another.

Perl is a relatively new language developed at JPL by Larry Walls that is gaining wide acceptance as an alternative to awk, sed and other commands. Perl is said to combine the best of

awk, sed, and other UNIX utilities to form a powerful text manipulation language. Perl runs on UNIX and Microsoft DOS and is distributed free of charge by the author in source form. Like awk, perl is primarily used for text manipulation.

For mission specific development, platform and vendor-specific scripting languages may be used. All of these languages are very powerful and can provide an easy way to perform difficult text manipulation tasks or process control tasks. The use of these scripting languages should be tempered by the knowledge that they may be cryptic, difficult to maintain, and not portable. They should not be used for general-purpose programming.

2.6.2 Tools

Tools are needed to support the process of software development. These tools range from computer aided software engineering (CASE) tools to assist in the design of the software to code generators to allow for the automatic creation of code from design outputs such as design drawings and screen layouts.

The importance of standards for tools is in the exchange of information between tools. Since vendors may come and go, it is important to be able reuse the outputs of one tool with another tool. Standards that are applicable to development tools are listed in Table 2-29.

Table 2-29. Development Tool Standards

ISO/IEC 13719, Portable Common Tool Environment (PCTE) Application Programmer's Interface
X/Open Publication Set T408, XCDE Definitions, Infrastructure, Services and Applications Set
Windows 95
CDIF 1994 Interim Standard, consisting of Overview (EIA/IS-106, ISBN 0-7908-0012-8), Framework for Modeling and Extensibility (EIA/IS-107, ISBN 0-7908-0013-6), General Rules for Syntaxes and Encodings (EIA/IS-108, ISBN 0-7908-0014-4), SYNTAX.1 (EIA/IS-109, ISBN 0-7908-0015-2), ENCODING.1, (EIA/IS-110, ISBN 0-7908-0016-0), Foundation (EIA/IS-111, ISBN 0-7908-0017-9)

In the UNIX world, efforts are taking place within the X/Open community with the Portable Common Tools Environment (PCTE) and the Common Desktop Environment (CDE) for tool interoperability.

In the personal computer market, products that have the Windows 95 logo provide some level of interoperability through drag and drop interfaces. However, there is no guarantee that the data will be interchangeable over time. To guarantee interchangeability over time, data structure standards are needed. The same problems that prevail in the UNIX environment are found in the Windows environment.

The Electronic Industry Association (EIA) has published an interim standard for data interchange between CASE tools, the CASE Data Interchange Format (CDIF) as a means of exchanging

engineering diagrams between tools [Reference 3]. The CDIF Family of Standards provides a published set of vendor-independent, method-independent definitions for meta-data concepts, and for CASE data concepts in particular. The CDIF Family of Standards also defines standard ways of moving this information between tools, without the need for customized interfaces. This allows users to select the most appropriate tools and tool configurations for their organizations and their problem-domains.

The outputs of code generation tools has the most promise for data interchange. The output of most tools will be some language that can be compiled from a file. Tools selected should generate code in one of the approved languages (Smalltalk, C++, Ada 95, and C), with Smalltalk, C++, and Ada 95 being preferred.

Most of the standards listed above are supported by vendors, either with current products or as participants in the standardization process. However, not all standards are supported by any single vendor. Also, the standards do not address all of the issues involved in tool interoperability. Because of the incomplete nature of standards for development tools and the lack of widespread acceptance, no standards are recommended at this time, with the exception of the language standards. However, tools that are selected should comply with at least a subset of the standards listed.

2.6.3 Repository

To promote reuse, repositories of reusable components must be developed. There do not appear to be widely accepted standards for repositories. The DoD CARDS and DISA STARS projects have developed some internal standards, but these are primarily for documentation and contract data requirements lists (CDRL). It will be up to the development organization to select appropriate repository products, based on the compatibility of the repository with other tools selected.

2.6.4 Process

There are limited standards for development processes. Most methodologies are proprietary (for example, Booch, Coad & Yourdon). However, some standards have been developed for the analysis stages. The Integration Definition for Function Modeling (IDEF0) is an accepted FIPS for activity and process modeling. IDEF1X is also an accepted FIPS for data modeling. However, neither standard is widely supported by tools and they are not integrated with other development methodologies. The development organization should pick a methodology that is well documented and supported by automated tools.

3. Sources for Specifications and Information

The following sections list sources for further information about standards. All of these organizations provide at least some on-line information about the relevant standards. However, only a few, e.g., IETF, NIST and the CCSDS, provide full on-line information. Other organizations require the purchase of standards documents for detailed specifications. In addition to this section, the Renaissance World Wide Web (WWW) home page (http://joy.gsfc.nasa.gov/renhome/REN_home.html) lists the standards with hot links to the related WWW pages.

3.1. Accredited Standards Committee X3

World Wide Web Pages:

Home Page - http://www.x3.org/

SQL Standards Home Page - http://www.jcc.com/sql_stnd.html

SmallTalk FAQ - http://chip.cs.uiuc.edu/users/dnsmith/Smalltalk%20Implementations.html

3.2. American National Standards Institute

World Wide Web Pages:

Home Page - http://www.ansi.org/

Standards Information Databases - http://www.ansi.org/sid_top.html

3.3. CompuServe Incorporated

World Wide Web Pages:

Home Page - http://www.compuserve.com/ [Note: no explicit link to GIF information was found from this page.]

3.4. Consultative Committee for Space Data Systems (CCSDS)

World Wide Web Pages:

CCSDS Home Page - http://www.gsfc.nasa.gov/ccsds/ccsds_home.html

Code 500 Library - http://joy.gsfc.nasa.gov/CCSDS-A.html

3.5. Electronic Industry Association, Case Data Interchange Format (CDIF) Division

World Wide Web Pages:

Home Page: http://www.cdif.org/

Standards - http://www.cdif.org/standard1994.html

http://www.cdif.org/standard1991.html

3.6. International Electrotechnical Commission

World Wide Web Pages:

Home Page: http://www.hike.te.chiba-u.ac.jp/ikeda/IEC/home.html

3.7. International Organization for Standardization (ISO)

World Wide Web Pages:

Home Page: http://www.iso.ch/welcome.html

3.8. Internet Engineering Task Force (IETF)

World Wide Web Pages:

Home Page - http://www.ietf.cnri.reston.va.us/home.html

Index to RFCs - http://ds.internic.net/ds/dspg1intdoc.html

The standards set by the IETF are currently summarized in RFC 1920, November 1995. The tables of usable protocol standards are contained in Appendix A.

3.9. Institute of Electrical and Electronics Engineers, Inc. (IEEE)

World Wide Web Pages:

Home Page - http://www.ieee.org/

Standards - http://stdsbbs.ieee.org/

Computer Society - http://ada.computer.org:80/cshome.htm

3.10. International Telecommunications Union (ITU)

[Formerly the CCITT]

World Wide Web Pages:

Home Page - http://www.itu.ch/

3.11. Microsoft Corporation

World Wide Web Pages:

Home Page - http://www.microsoft.com/

3.12. National Center for Supercomputing Applications (NCSA)

World Wide Web Pages:

Home Page - http://www.ncsa.uiuc.edu/General/NCSAHome.html

3.13. National Institute for Standards and Technology (NIST)

World Wide Web Pages:

Home Page - http://www.nist.gov/

Computer Systems Laboratory (CSL) - http://www.ncsl.nist.gov/

CSL information search engine - http://dsys.ncsl.nist.gov/nssn/search/index.html

CSL FIPS standards index - http://www.ncsl.nist.gov/fips/index.html

FIPS CSL list - http://www.ncsl.nist.gov/fipslist/index.html

3.14. National Space Science Data Center (NSSDC)

World Wide Web Pages:

Home Page - http://nssdc.gsfc.nasa.gov/

CDF Page - http://nssdc.gsfc.nasa.gov/cdf/cdf_home.html

3.15. National Weather Service

World Wide Web Pages:

Home Page - http://www.noaa.gov/nws/nws_intro.html

3.16. Object Data Management Group (ODMG)

World Wide Web Pages:

Home Page - http://www.odmg.org/welcome.html

Standards - http://www.odmg.org/odmg-93.html

3.17. Object Management Group (OMG)

World Wide Web Pages:

Home Page - http://www.omg.org/

Web Server Contents index - http://ruby.omg.org/content.htm

3.18. Open Information Interchange (OII)

World Wide Web Pages:

Home Page - http://www.echo.lu./home.html

OII Standards page - http://www.echo.lu./impact/oii/oiistand.html

Raster Graphics standards index - http://www.echo.lu./impact/oii/raster.html

Related graphics pages - http://www.dcs.ed.ac.uk/%7Emxr/gfx/index.html, University of Edinburgh

3.19. Open Software Foundation

World Wide Web Pages:

Home Page - http://www.osf.org/

DCE page - http://www.osf.org/dce/index.html

Motif page - http://www.osf.org/motif/index.html

3.20. SUN Microsystems

World Wide Web Pages:

Home Page - http://www.sun.com/

Java Page - http://java.sun.com/

3.21. World Meteorological Organization

World Wide Web Pages:

Home Page - http://www.wmo.ch

3.22. X/Open

World Wide Web Pages:

Home Page - http://www.xopen.org/

Public Information Server - http://www.xopen.co.uk/infosrv/

Publications - http://www.xopen.co.uk/public/pubs/index.htm (The Single UNIX Specification is a publication available via this page)

Appendix A. IETF RFC Summary

This appendix contains the listing of Internet Engineering Task Force (IETF) Request For Comments (RFC) as listed in RFC 1920 Internet Standards November 1995. Each table lists the protocol that the RFC addresses, the title of the RFC, the status of the RFC, the RFC number, and for the standard protocols, indicates the larger grouping of which it is a part. The status of an RFC may be Required (Req), Recommended (Rec), Elective (Elec), or Proposed (Prop). The complete text of RFC 1920 can be found on the World Wide Web at the IETF's Index to RFCs page (http://ds.internic.net/ds/dspg1intdoc.html). This memo also contains information on the IETF standardization process. The IETF publishes a superseding version to this RFC (with a different RFC number) on a regular basis to keep it current. The current edition is available at the ITEF's Index to RFC's Web page.

A.1 Standard Protocols (RFC 1920 Section 6.2)

Table A-1. Standard Protocols

Protocol	Name	Status	RFC	STD
--------	Internet Official Protocol Standards	Req	1920	1
--------	Assigned Numbers	Req	1700	2
--------	Host Requirements - Communications	Req	1122	3
--------	Host Requirements - Applications	Req	1123	3
IP	Internet Protocol	Req	791	5
	as amended by:--------			
--------	IP Subnet Extension	Req	950	5
--------	IP Broadcast Datagrams	Req	919	5
--------	IP Broadcast Datagrams with Subnets	Req	922	5
ICMP	Internet Control Message Protocol	Req	792	5
IGMP	Internet Group Multicast Protocol	Rec	1112	5
UDP	User Datagram Protocol	Rec	768	6
TCP	Transmission Control Protocol	Rec	793	7
TELNET	Telnet Protocol	Rec	854,855	8
FTP	File Transfer Protocol	Rec	959	9
SMTP	Simple Mail Transfer Protocol	Rec	821	10
SMTP-SIZE	SMTP Service Ext for Message Size	Rec	1870	10
SMTP-EXT	SMTP Service Extensions	Rec	1869	10
MAIL	Format of Electronic Mail Messages	Rec	822	11
CONTENT	Content Type Header Field	Rec	1049	11
NTPV2	Network Time Protocol (Version 2)	Rec	1119	12
DOMAIN	Domain Name System	Rec	1034,1035	13
DNS-MX	Mail Routing and the Domain System	Rec	974	14
SNMP	Simple Network Management Protocol	Rec	1157	15
SMI	Structure of Management Information	Rec	1155	16
Concise-MIB	Concise MIB Definitions	Rec	1212	16
MIB-II	Management Information Base-II	Rec	1213	17
NETBIOS	NetBIOS Service Protocols	Ele	1001,1002	19
ECHO	Echo Protocol	Rec	862	20
DISCARD	Discard Protocol	Ele	863	21
CHARGEN	Character Generator Protocol	Ele	864	22
QUOTE	Quote of the Day Protocol	Ele	865	23
USERS	Active Users Protocol	Ele	866	24
DAYTIME	Daytime Protocol	Ele	867	25
TIME	Time Server Protocol	Ele	868	26
TFTP	Trivial File Transfer Protocol	Ele	1350	33
TP-TCP	ISO Transport Service on top of the TCP	Ele	1006	35
ETHER-MIB	Ethernet MIB	Ele	1643	50
PPP	Point-to-Point Protocol (PPP)	Ele	1661	51
PPP-HDLC	PPP in HDLC Framing	Ele	1662	51
IP-SMDS	IP Datagrams over the SMDS Service	Ele	1209	52

A.2 Network-Specific Standard Protocols (RFC 1920 Section 6.3)

All Network-Specific Standards have Elective status.

Table A-2. Network-Specific Standard Protocols

Protocol	Name	State	RFC	STD
IP-ATM	Classical IP and ARP over ATM	Prop	1577	
IP-FR	Multiprotocol over Frame Relay	Draft	1490	
ATM-ENCAP	Multiprotocol Encapsulation over ATM	Prop	1483	
IP-TR-MC	IP Multicast over Token-Ring LANs	Prop	1469	
IP-FDDI	Transmission of IP and ARP over FDDI Net	Std	1390	36
IP-HIPPI	IP and ARP on HIPPI	Prop	1374	
IP-X.25	X.25 and ISDN in the Packet Mode	Draft	1356	
IP-FDDI	Internet Protocol on FDDI Networks	Draft	1188	
ARP	Address Resolution Protocol	Std	826	37
RARP	A Reverse Address Resolution Protocol	Std	903	38
IP-ARPA	Internet Protocol on ARPANET	Std	BBN1822	39
IP-WB	Internet Protocol on Wideband Network	Std	907	40
IP-E	Internet Protocol on Ethernet Networks	Std	894	41
IP-EE	Internet Protocol on Exp. Ethernet Nets	Std	895	42
IP-IEEE	Internet Protocol on IEEE 802	Std	1042	43
IP-DC	Internet Protocol on DC Networks	Std	891	44
IP-HC	Internet Protocol on Hyperchannel	Std	1044	45
IP-ARC	Transmitting IP Traffic over ARCNET Nets	Std	1201	46
IP-SLIP	Transmission of IP over Serial Lines	Std	1055	47
IP-NETBIOS	Transmission of IP over NETBIOS	Std	1088	48
IP-IPX	Transmission of 802.2 over IPX Networks	Std	1132	49

A.3 Draft Standard Protocols (RFC 1920 Section 6.4)

Table A-3. Draft Standard Protocols

Protocol	Name	Status	RFC
COEX-MIB	Coexistence between SNMPV1 & SNMPV2	Elective	1908
SNMPv2-MIB	MIB for SNMPv2	Elective	1907
TRANS-MIB	Transport Mappings for SNMPv2	Elective	1906
OPS-MIB	Protocol Operations for SNMPv2	Elective	1905
CONF-MIB	Conformance Statements for SNMPv2	Elective	1904
CONV-MIB	Textual Conventions for SNMPv2	Elective	1903
SMIV2	SMI for SNMPv2	Elective	1902
CON-MD5	Content-MD5 Header Field	Elective	1864
OSPF-MIB	OSPF Version 2 MIB	Elective	1850
STR-REP	String Representation ...	Elective	1779
X.500syn	X.500 String Representation ...	Elective	1778
X.500lite	X.500 Lightweight ...	Elective	1777
BGP-4-APP	Application of BGP-4	Elective	1772
BGP-4	Border Gateway Protocol 4	Elective	1771
PPP-DNCP	PPP DECnet Phase IV Control Protocol	Elective	1762
RMON-MIB	Remote Network Monitoring MIB	Elective	1757
802.5-MIB	IEEE 802.5 Token Ring MIB	Elective	1748
BGP-4-MIB	BGP-4 MIB	Elective	1657
POP3	Post Office Protocol, Version 3	Elective	1725
RIP2-MIB	RIP Version 2 MIB Extension	Elective	1724
RIP2	RIP Version 2-Carrying Additional Info.	Elective	1723
RIP2-APP	RIP Version 2 Protocol App. Statement	Elective	1722
SIP-MIB	SIP Interface Type MIB	Elective	1694
-------	Def Man Objs Parallel-printer-like	Elective	1660
-------	Def Man Objs RS-232-like	Elective	1659
-------	Def Man Objs Character Stream	Elective	1658
SMTP-8BIT	SMTP Service Ext or 8bit-MIMEtransport	Elective	1652
OSI-NSAP	Guidelines for OSI NSAP Allocation	Elective	1629
OSPF2	Open Shortest Path First Routing V2	Elective	1583
ISO-TS-ECHO	Echo for ISO-8473	Elective	1575
DECNET-MIB	DECNET MIB	Elective	1559
-------	Message Header Ext. of Non-ASCII Text	Elective	1522
MIME	Multipurpose Internet Mail Extensions	Elective	1521
802.3-MIB	IEEE 802.3 Repeater MIB	Elective	1516
BRIDGE-MIB	BRIDGE-MIB	Elective	1493
NTPV3	Network Time Protocol (Version 3)	Elective	1305
IP-MTU	Path MTU Discovery	Elective	1191
FINGER	Finger Protocol	Elective	1288
BOOTP	Bootstrap Protocol	Recommended	951,1497
NICNAME	WhoIs Protocol	Elective	954

A.4 Proposed Standard Protocols (RFC 1920 Section 6.5)

Table A-4. Proposed Standard Protocols

Protocol	Name	Status	RFC
WHOIS++M	How to Interact with a Whois++ Mesh	Elective	1914
WHOIS++A	Architecture of Whois++ Index Service	Elective	1913
DSN	Delivery Status Notifications	Elective	1894
EMS-CODE	Enhanced Mail System Status Codes	Elective	1893
MIME-RPT	Multipart/Report	Elective	1892
SMTP-DSN	SMTP Delivery Status Notifications	Elective	1891
RTP-AV	RTP Audio/Video Profile	Elective	1890
RTP	Transport Protocol for Real-Time Apps	Elective	1889
DNS-IPV6	DNS Extensions to support IPv6	Elective	1886
ICMPv6	ICMPv6 for IPv6	Elective	1885
IPV6-Addr	IPv6 Addressing Architecture	Elective	1884
IPV6	IPv6 Specification	Elective	1883
HTML	Hypertext Markup Language - 2.0	Elective	1866
SMTP-Pipe	SMTP Serv. Ext. for Command Pipelining	Elective	1854
MIME-Sec	MIME Object Security Services	Elective	1848
MIME-Encyp	MIME: Signed and Encrypted	Elective	1847
WHOIS++	Architecture of the WHOIS++ service	Elective	1835
--------	Binding Protocols for ONC RPC Version 2	Elective	1833
XDR	External Data Representation Standard	Elective	1832
RPC	Remote Procedure Call Protocol V. 2	Elective	1831
--------	ESP DES-CBC Transform	Ele/Req	1829
--------	IP Authentication using Keyed MD5	Ele/Req	1828
ESP	IP Encapsulating Security Payload	Ele/Req	1827
IPV6-AH	IP Authentication Header	Ele/Req	1826
--------	Security Architecture for IP	Ele/Req	1825
RREQ	Requirements for IP Version 4 Routers	Elective	1812
URL	Relative Uniform Resource Locators	Elective	1808
CLDAP	Connection-less LDAP	Elective	1798
OSPF-DC	Ext. OSPF to Support Demand Circuits	Elective	1793
TMUX	Transport Multiplexing Protocol	Elective	1692
TFTP-Opt	TFTP Options	Elective	1784
TFTP-Blk	TFTP Blocksize Option	Elective	1783
TFTP-Ext	TFTP Option Extension	Elective	1782
OSI-Dir	OSI User Friendly Naming ...	Elective	1781
MIME-EDI	MIME Encapsulation of EDI Objects	Elective	1767
Lang-Tag	Tags for Identification of Languages	Elective	1766
XNSCP	PPP XNS IDP Control Protocol	Elective	1764
BVCP	PPP Banyan Vines Control Protocol	Elective	1763
Print-MIB	Printer MIB	Elective	1759
ATM-SIG	ATM Signaling Support for IP over ATM	Elective	1755
IPNG	Recommendation for IP Next Generation	Elective	1752
802.5-SSR	802.5 SSR MIB using SMIv2	Elective	1749
SDLCSMIv2	SNADLC SDLC MIB using SMIv2	Elective	1747
BGP4/IDRP	BGP4/IDRP for IP/OSPF Interaction	Elective	1745
AT-MIB	Appletalk MIB	Elective	1742
MacMIME	MIME Encapsulation of Macintosh files	Elective	1740
URL	Uniform Resource Locators	Elective	1738
POP3-AUTH	POP3 AUTHentication command	Elective	1734

Protocol	Name	Status	RFC
IMAP4-AUTH	IMAP4 Authentication Mechanisms	Elective	1731
IMAP4	Internet Message Access Protocol V4	Elective	1730
PPP-MP	PPP Multilink Protocol	Elective	1717
RDBMS-MIB	RDMS MIB - using SMIv2	Elective	1697
MODEM-MIB	Modem MIB - using SMIv2	Elective	1696
ATM-MIB	ATM Management Version 8.0 using SMIv2	Elective	1695
SNANAU-MIB	SNA NAUs MIB using SMIv2	Elective	1665
PPP-TRANS	PPP Reliable Transmission	Elective	1663
BGP-4-IMP	BGP-4 Roadmap and Implementation	Elective	1656
--------	Postmaster Convention X.400 Operations	Elective	1648
TN3270-En	TN3270 Enhancements	Elective	1647
PPP-BCP	PPP Bridging Control Protocol	Elective	1638
UPS-MIB	UPS Management Information Base	Elective	1628
AAL5-MTU	Default IP MTU for use over ATM AAL5	Elective	1626
PPP-SONET	PPP over SONET/SDH	Elective	1619
PPP-ISDN	PPP over ISDN	Elective	1618
DNS-R-MIB	DNS Resolver MIB Extensions	Elective	1612
DNS-S-MIB	DNS Server MIB Extensions	Elective	1611
FR-MIB	Frame Relay Service MIB	Elective	1604
PPP-X25	PPP in X.25	Elective	1598
OSPF-NSSA	The OSPF NSSA Option	Elective	1587
OSPF-Multi	Multicast Extensions to OSPF	Elective	1584
SONET-MIB	MIB SONET/SDH Interface Type	Elective	1595
RIP-DC	Extensions to RIP to Support Demand Cir.	Elective	1582
--------	Evolution of the Interfaces Group of MIB-II	Elective	1573
PPP-LCP	PPP LCP Extensions	Elective	1570
X500-MIB	X.500 Directory Monitoring MIB	Elective	1567
MAIL-MIB	Mail Monitoring MIB	Elective	1566
NSM-MIB	Network Services Monitoring MIB	Elective	1565
CIPX	Compressing IPX Headers Over WAM Media	Elective	1553
IPXCP	PPP Internetworking Packet Exchange Control	Elective	1552
DHCP-BOOTP	Interoperation Between DHCP and BOOTP	Elective	1534
DHCP-BOOTP	DHCP Options and BOOTP Vendor Extensions	Elective	1533
BOOTP	Clarifications and Extensions BOOTP	Elective	1532
DHCP	Dynamic Host Configuration Protocol	Elective	1541
SRB-MIB	Source Routing Bridge MIB	Elective	1525
CIDR-STRA	CIDR Address Assignment...	Elective	1519
CIDR-ARCH	CIDR Architecture...	Elective	1518
CIDR-APP	CIDR Applicability Statement	Elective	1517
--------	802.3 MAU MIB	Elective	1515
HOST-MIB	Host Resources MIB	Elective	1514
--------	Token Ring Extensions to RMON MIB	Elective	1513
FDDI-MIB	FDDI Management Information Base	Elective	1512
KERBEROS	Kerberos Network Authentication Ser (V5)	Elective	1510
GSSAPI	Generic Security Service API: C-bindings	Elective	1509
GSSAPI	Generic Security Service Application...	Elective	1508
DASS	Distributed Authentication Security...	Elective	1507
--------	X.400 Use of Extended Character Sets	Elective	1502
HARPOON	Rules for Downgrading Messages...	Elective	1496
Mapping	MHS/RFC-822 Message Body Mapping	Elective	1495
Equiv	X.400/MIME Body Equivalences	Elective	1494
IDPR	Inter-Domain Policy Routing Protocol	Elective	1479
IDPR-ARCH	Architecture for IDPR	Elective	1478
PPP/Bridge	MIB Bridge PPP MIB	Elective	1474
PPP/IP MIB	IP Network Control Protocol of PPP MIB	Elective	1473

Protocol	Name	Status	RFC
PPP/SEC MIB	Security Protocols of PPP MIB	Elective	1472
PPP/LCP MIB	Link Control Protocol of PPP MIB	Elective	1471
X25-MIB	Multiprotocol Interconnect on X.25 MIB	Elective	1461
SNMPv2	Coexistence between SNMPv1 and SNMPv2	Elective	1452
SNMPv2	Management Information Base for SNMPv2	Elective	1450
SNMPv2	Transport Mappings for SNMPv2	Elective	1449
SNMPv2	Protocol Operations for SNMPv2	Elective	1448
SNMPv2	Conformance Statements for SNMPv2	Elective	1444
SNMPv2	Textual Conventions for SNMPv2	Elective	1443
SNMPv2	SMI for SNMPv2	Elective	1442
SNMPv2	Introduction to SNMPv2	Elective	1441
PEM-KEY	PEM - Key Certification	Elective	1424
PEM-ALG	PEM - Algorithms, Modes, and Identifiers	Elective	1423
PEM-CKM	PEM - Certificate-Based Key Management	Elective	1422
PEM-ENC	PEM - Message Encryption and Auth	Elective	1421
SNMP-IPX	SNMP over IPX	Elective	1420
SNMP-AT	SNMP over AppleTalk	Elective	1419
SNMP-OSI	SNMP over OSI	Elective	1418
FTP-FTAM	FTP-FTAM Gateway Specification	Elective	1415
IDENT-MIB	Identification MIB	Elective	1414
IDENT	Identification Protocol	Elective	1413
DS3/E3-MIB	DS3/E3 Interface Type	Elective	1407
DS1/E1-MIB	DS1/E1 Interface Type	Elective	1406
BGP-OSPF	BGP OSPF Interaction	Elective	1403
--------	Route Advertisement In BGP2 And BGP3	Elective	1397
SNMP-X.25	SNMP MIB Extension for X.25 Packet Layer	Elective	1382
SNMP-LAPB	SNMP MIB Extension for X.25 LAPB	Elective	1381
PPP-ATCP	PPP AppleTalk Control Protocol	Elective	1378
PPP-OSINLCP	PPP OSI Network Layer Control Protocol	Elective	1377
TABLE-MIB	IP Forwarding Table MIB	Elective	1354
SNMP-PARTY-MIB	Administration of SNMP	Elective	1353
SNMP-SEC	SNMP Security Protocols	Elective	1352
SNMP-ADMIN	SNMP Administrative Model	Elective	1351
TOS	Type of Service in the Internet	Elective	1349
PPP-AUTH	PPP Authentication	Elective	1334
PPP-LINK	PPP Link Quality Monitoring	Elective	1333
PPP-IPCP	PPP Control Protocol	Elective	1332
-------	X.400 1988 to 1984 downgrading	Elective	1328
-------	Mapping between X.400(1988)	Elective	1327
TCP-EXT	TCP Extensions for High Performance	Elective	1323
FRAME-MIB	Management Information Base for Frame	Elective	1315
NETFAX	File Format for the Exchange of Images	Elective	1314
IARP	Inverse Address Resolution Protocol	Elective	1293
FDDI-MIB	FDDI-MIB	Elective	1285
-------	Encoding Network Addresses	Elective	1277
-------	Replication and Distributed Operations	Elective	1276
-------	COSINE and Internet X.500 Schema	Elective	1274
BGP-MIB	Border Gateway Protocol MIB (Version 3)	Elective	1269
ICMP-ROUT	ICMP Router Discovery Messages	Elective	1256
IPSO	DoD Security Options for IP	Elective	1108
OSI-UDP	OSI TS on UDP	Elective	1240
STD-MIBs	Reassignment of Exp MIBs to Std MIBs	Elective	1239
IPX-IP	Tunneling IPX Traffic through IP Nets	Elective	1234
GINT-MIB	Extensions to the Generic-Interface MIB	Elective	1229
IS-IS	OSI IS-IS for TCP/IP Dual Environments	Elective	1195

Protocol	Name	Status	RFC
IP-CMPRS	Compressing TCP/IP Headers	Elective	1144
NNTP	Network News Transfer Protocol	Elective	977

A.5 Experimental Protocols (RFC 1920 Section 6.7)

All Experimental protocols have the Limited Use status.

Table A-5. Experimental Protocols

Protocol	Name	RFC
MIME-VP	Voice Profile for Internet Mail	1911
SNMPV2SM	User-based Security Model for SNMPv2	1910
SNMPV2AI	SNMPv2 Administrative Infrastructure	1909
SNMPV2CB	Introduction to Community-based SNMPv2	1901
-------	IPv6 Testing Address Allocation	1897
DNS-LOC	Location Information in the DNS	1876
SGML-MT	SGML Media Types	1874
CONT-MT	Access Type Content-ID	1873
RELAT-MT	Multipart/Related	1872
UNARP	ARP Extension - UNARP	1868
-------	Form-based File Upload in HTML	1867
-------	BGP/IDRP Route Server Alternative	1863
-------	IP Authentication using Keyed SHA	1852
ESP3DES	ESP Triple DES Transform	1851
-------	SMTP 521 Reply Code	1846
-------	SMTP Serv. Ext. for Checkpoint/Restart	1845
-------	X.500 Mapping X.400 and RFC 822 Addresses	1838
-------	Tables and Subtrees in the X.500 Directory	1837
-------	O/R Address hierarchy in X.500	1836
-------	SMTP Serv. Ext. Large and Binary MIME Msgs.	1830
ST2	Stream Protocol Version 2	1819
-------	Content-Disposition Header	1806
-------	Schema Publishing in X.500 Directory	1804
-------	X.400-MHS use X.500 to support X.400-MHS Routing	1801
-------	Class A Subnet Experiment	1797
TCP/IPXMIB	TCP/IPX Connection Mib Specification	1792
-------	TCP And UDP Over IPX Networks With Fixed Path MTU	1791
ICMP-DM	ICMP Domain Name Messages	1788
CLNP-MULT	Host Group Extensions for CLNP Multicasting	1768
OSPF-OVFL	OSPF Database Overflow	1765
RWP	Remote Write ProtocolL - Version 1.0	1756
NARP	NBMA Address Resolution Protocol	1735
DNS-DEBUG	Tools for DNS debugging	1713
DNS-ENCODE	DNS Encoding of Geographical Location	1712
TCP-POS	An Extension to TCP: Partial Order Service	1693
-------	DNS to Distribute RFC1327 Mail Address Mapping Tables	1664
T/TCP	TCP Extensions for Transactions	1644
UTF-7	A Mail-Safe Transformation Format of Unicode	1642
MIME-UNI	Using Unicode with MIME	1641
FOOBAR	FTP Operation Over Big Address Records	1639
X500-CHART	Charting Networks in the X.500 Directory	1609
X500-DIR	Representing IP Information in the X.500 Directory	1608
SNMP-DPI	SNMP Distributed Protocol Interface	1592
CLNP-TUBA	Use of ISO CLNP in TUBA Environments	1561
REM-PRINT	TPC.INT Subdomain Remote Printing - Technical	1528
EHF-MAIL	Encoding Header Field for Internet Messages	1505

Protocol	Name	RFC
REM-PRT	An Experiment in Remote Printing	1486
RAP	Internet Route Access Protocol	1476
TP/IX	TP/IX: The Next Internet	1475
X400	Routing Coordination for X.400 Services	1465
DNS	Storing Arbitrary Attributes in DNS	1464
IRCP	Internet Relay Chat Protocol	1459
TOS-LS	Link Security TOS	1455
SIFT/UFT	Sender-Initiated/Unsolicited File Transfer	1440
DIR-ARP	Directed ARP	1433
TEL-SPX	Telnet Authentication: SPX	1412
TEL-KER	Telnet Authentication: Kerberos V4	1411
MAP-MAIL	X.400 Mapping and Mail-11	1405
TRACE-IP	Traceroute Using an IP Option	1393
DNS-IP	Experiment in DNS Based IP Routing	1383
RMCP	Remote Mail Checking Protocol	1339
TCP-HIPER	TCP Extensions for High Performance	1323
MSP2	Message Send Protocol 2	1312
DSLCP	Dynamically Switched Link Control	1307
--------	X.500 and Domains	1279
IN-ENCAP	Internet Encapsulation Protocol	1241
CLNS-MIB	CLNS-MIB	1238
CFDP	Coherent File Distribution Protocol	1235
SNMP-DPI	SNMP Distributed Program Interface	1228
IP-AX.25	IP Encapsulation of AX.25 Frames	1226
ALERTS	Managing Asynchronously Generated Alerts	1224
MPP	Message Posting Protocol	1204
SNMP-BULK	Bulk Table Retrieval with the SNMP	1187
DNS-RR	New DNS RR Definitions	1183
IMAP2	Interactive Mail Access Protocol	1176
NTP-OSI	NTP over OSI Remote Operations	1165
DMF-MAIL	Digest Message Format for Mail	1153
RDP	Reliable Data Protocol	908,1151
TCP-ACO	TCP Alternate Checksum Option	1146
IP-DVMRP	IP Distance Vector Multicast Routing	1075
VMTP	Versatile Message Transaction Protocol	1045
COOKIE-JAR	Authentication Scheme	1004
NETBLT	Bulk Data Transfer Protocol	998
IRTP	Internet Reliable Transaction Protocol	938
LDP	Loader Debugger Protocol	909
RLP	Resource Location Protocol	887
NVP-II	Network Voice Protocol	ISI-memo
PVP	Packet Video Protocol	ISI-memo

A.6 Informational Protocols (RFC 1920 Section 6.8)

Information protocols have no status.

Table A-6. Informational Protocols

Protocol	Name	RFC
CYBERCASH	CyberCash Credit Card Protocol Version 0.8	1898
--------	text/enriched MIME Content-type	1896
--------	Application/CALS-1840 Content-type	1895
--------	PPP IPCP Extensions for Name Server Addresses	1877
SNPP	Simple Network Paging Protocol - Version 2	1861
--------	ISO Transport Class 2 Non-use Explicit Flow Control over TCP RFC1006 extension	1859
--------	IP in IP Tunneling	1853
--------	PPP Network Control Protocol for LAN Extension	1841
TESS	The Exponential Security System	1824
NFSV3	NFS Version 3 Protocol Specification	1813
--------	A Format for Bibliographic Records	1807
SDMD	IPv4 Option for Sender Directed MD Delivery	1770
SNTP	Simple Network Time Protocol	1769
SNOOP	Snoop Version 2 Packet Capture File Format	1761
BINHEX	MIME Content Type for BinHex Encoded Files	1741
RWHOIS	Referral Whois Protocol	1714
DNS-NSAP	DNS NSAP Resource Records	1706
RADIO-PAGE	TPC.INT Subdomain: Radio Paging -- Technical Procedures	1703
GRE-IPv4	Generic Routing Encapsulation over IPv4	1702
GRE	Generic Routing Encapsulatio	1701
IPXWAN	Novell IPX Over Various WAN Media	1634
ADSNA-IP	Advanced SNA/IP: A Simple SNA Transport Protocol	1538
AUBR	Appletalk Update-Based Routing Protocol...	1504
TACACS	Terminal Access Control Protocol	1492
SUN-NFS	Network File System Protocol	1094
SUN-RPC	Remote Procedure Call Protocol Version 2	1057
GOPHER	The Internet Gopher Protocol	1436
-------	Data Link Switching: Switch-to-Switch Protocol	1434
LISTSERV	Listserv Distribute Protocol	1429
-------	Replication Requirements	1275
PCMAIL	Pcmail Transport Protocol	1056
MTP	Multicast Transport Protocol	1301
BSD Login	BSD Login	1282
DIXIE	DIXIE Protocol Specification	1249
IP-X.121	IP to X.121 Address Mapping for DDN	1236
OSI-HYPER	OSI and LLC1 on HYPERchannel	1223
HAP2	Host Access Protocol	1221
SUBNETASGN	On the Assignment of Subnet Numbers	1219
SNMP-TRAPS	Defining Traps for use with SNMP	1215
DAS	Directory Assistance Service	1202
MD4	MD4 Message Digest Algorithm	1186

Appendix B. Consolidated Standards Table

B.1. Communications Standards

	Mission Integration	Development
Global	Host Requirements - Communications, RFC 1122 Host Requirements - Applications, RFC1123 Internet protocol, RFCs 791, 950, 919, 922 Internet Control Message Protocol, RFC792 Internet Group Multicast Protocol, RFC1112 User Datagram Protocol, RFC 768 Transmission Control Protocol, RFC 793 Routing Information Protocol, RFC 1058 Profiles for Open Systems Internetworking Technologies (POSIT), FIPS PUB 146-2	Recommendation for IP Next Generation (IPv6), RFC 1752 RIP Version 2 - Carrying Additional Information, RFC1723 Open Shortest Path First Routing (OSPF), Version 2, RFC1583 Point to Point Protocol (PPP), RFC 1661 Transmission of IP over Serial Lines, RFC1055 Classical IP and ARP over ATM, RFC1577 Multiprotocol over Frame Relay, RFC1490 Multiprotocol Encapsulation over ATM, RFC 1483 Transmission of IP and ARP over FDDI Net, RFC 1390 Internet Protocol on FDDI Networks, RFC 1188 Address Resolution Protocol, RFC 826 A Reverse Address Resolution Protocol, RFC 903 Internet Protocol on Wideband Network, RFC 907 Internet Protocol on Ethernet Networks, RFC 894 Internet Protocol on Exp. Ethernet Nets, RFC 895 ISO Transport Service on top of the TCP, RFC1006 Packet Telemetry, CCSDS 102.0-B-3 Telecommand Part 1- Channel Service, CCSDS 201.0-B-1 Telecommand Part 2 - Data Routing Service, CCSDS 202.0-B-2

	Mission Integration	Development
Mission Specific	IP Multicast over Token-Ring LANs, RFC1469 IP and ARP on HIPPI, RFC 1374 X.25 and ISDN in the Packet Mode, RFC1356 Internet Protocol on IEEE 802, RFC1042 Transmission of IP over Serial Lines, RFC 1055 Transmission of 802.2 over IPX Networks, RFC 1132 Telemetry Summary of Concept and Rationale, CCSDS 100.0-G-1 Telecommand Summary of Concept and Service, CCSDS 200.0-G-6	Advanced Orbiting Systems (AOS), Networks and Data Links, CCSDS 701.0-B-2 Telecommand Part 2.1 - Command Operation Procedures, CCSDS 202.1-B-1 Telecommand Part 3 - Data Management Service, CCSDS 203.0-B-1

B.2. System Management

	Mission Integration	Development
Global	Simple Network Management Protocol, RFC 1157 Structure of Management Information, RFC 1155 Concise MIB Definitions, RFC 1212 Management Information Base-II, RFC1213	X/Open Management Protocols API (XMP), X/Open CAE Specification C306, ISBN 1-85912-027-X X/Open Management Protocols Profile (XMPP), X/Open CAE Specification C206, ISBN 1-85912-018-O X/Open Managed Objects Guide, X/Open Guide G302 ISBN 1-85912-006-7, 9/93 Common Management Information Protocol (CMIP), ISO9596 Remote Network Monitoring MIB, RFC1757 Ethernet MIB, RFC 1643 Government Network Management Profile (GNMP), FIPS PUB 179-1

	Mission Integration	Development
Mission Specific	IEEE 802.5 Token Ring MIB, RFC 1748 IEEE 802.3 Repeater MIB, RFC 1516 BRIDGE-MIB, RFC 1493 Printer MIB, RFC 1759 MIB SONET/SDH Interface Type, RFC1595 MIB Bridge PPP MIB, RFC1474 Multiprotocol Interconnect on X.25 MIB, RFC1461 SNMP MIB Extension for X.25 Packet Layer, RFC 1382 IP Forwarding Table MIB, RFC1354 Management Information Base for Frame Relay, RFC1315 Frame Relay Service MIB, RFC1604 RDMS MIB - using SMIv2, RFC1697 DNS Resolver MIB Extensions, RFC1612 DNS Server MIB Extensions, RFC1611 Coexistence between SNMPv1 and SNMPv2, RFC1452 Manager-to-Manager MIB, RFC1451 Management Information Base for SNMPv2, RFC1450 Transport Mappings for SNMPv2, RFC1449 Protocol Operations for SNMPv2, RFC1448 Party MIB for SNMPv2, RFC1447 Security Protocols for SNMPv2, RFC1446 Administrative Model for SNMPv2, RFC1445 Conformance Statements for SNMPv2, RFC1444 Textual Conventions for SNMPv2, RFC1443 SMI for SNMPv2, RFC1442 Introduction to SNMPv2, RFC1441	SNMP Distributed Program Interface, RFC1228 MIB Administration of SNMP, RFC1353 SNMP Security Protocols, RFC1352 SNMP Administrative Model, RFC1351 Host Resources MIB, RFC1514 X.500 Directory Monitoring MIB, RFC1567 Mail Monitoring MIB, RFC1566 Modem MIB - using SMIv2, RFC1696 IP Network Control Protocol of PPP MIB, RFC1473 Security Protocols of PPP MIB, RFC1472 Link Control Protocol of PPP MIB, RFC1471 FDDI Management Information Base, RFC1512 FDDI-MIB, RFC1285 ATM Management Version 8.0 using SMIv2, RFC1695 Network Services Monitoring MIB, RFC1565 Source Routing Bridge MIB, RFC1525

B.3. Security

	Mission Integration	Development
Global		ESP DES-CBC Transform, RFC1829 IP Authentication using Keyed MD5, RFC1828 IP Encapsulating Security Payload, RFC1827 IP Authentication Header, RFC1826 Security Architecture for IP, RFC1825 Kerberos Network Authentication Service (V5), RFC1510 Generic Security Service API: C-bindings, RFC1509 Generic Security Service Application Program Interface, RFC1508 Distributed Authentication Security Service, RFC1507 Directory Authentication Framework, CCITT X.509 OSF Distributed Computing Environment (DCE)
Mission Specific	Digital Signature Standard (DSS), FIPS PUB 186	Generic Security Service Application Program Interface, Version 2 (DRAFT) SOCKS Protocol Version 5 (DRAFT) Usename/Password Authentication for SOCKS V5 (DRAFT) GSS-API Authentication Method for SOCKS V5 (DRAFT) S/WAN Toolkit, RSA Data Security, Inc.

B.4. Network Transparency

	Mission Integration	Development
Global	Domain Name System, RFC1034, RFC1035 File Transfer Protocol (FTP), RFC 959	OSF Distributed Computing Environment (DCE) X/Open DCE: Directory Services, X/Open CAE Specification C312 ISBN 1-85912-078-4, 12/94 ISO/CCITT X.500 Directory Services Network File System Protocol, RFC1094 (Informational) NFS Version 3 Protocol Specification, RFC1813 (Informational) Protocols for X/Open Internetworking: XNFS, Issue 4, X/Open CAE Specification C218 ISBN 1-872630-66-9 (pending IEEE TFA approval) X/Open DCE: Remote Procedure Call, X/Open CAE Specification C309 ISBN 1-85912-041-5, 8/94 NIST Draft OSF Distributed Computing Environment (DCE) Remote Procedure Call (RPC) Component OMG CORBA 1.2, Object Management Group's Common Object Request Broker Architecture OMG CORBA 2.0, Object Management Group's Common Object Request Broker Architecture X/Open DCE: Time Services, X/Open CAE Specification C310 ISBN 1-85912-067-9, 11/94 Network Time Protocol (Version 2), RFC1119 Telnet Protocol Specification, RFC 854
Mission Specific	NetWare Directory Services (NetWare 4.1), Novell	FTP Operation Over Big Address Records, RFC 1639 Binding Protocols for ONC RPC Version 2, RFC1833 Telnet Authentication: Kerberos V4, RFC 1411

B.5. Network Applications, Email

	Mission Integration	Development
Global	Simple Mail Transfer Protocol, RFC821 SMTP Service Ext for Message Size, RFC1870 SMTP Service Extensions, RFC1869 Multipurpose Internet Mail Extensions (MIME), RFC1521 Format of Electronic Mail Messages, TFC822 Content Tupe Header Field, RFC1049	PEM - Key Certification, RFC1424 PEM - Algorithms, Modes, and Identifiers, RFC1423 PEM - Certificate-Based Key Management, RFC1422 PEM - Message Encryption and Authentication, RFC1421 MIME Object Security Services, RFC1848 MIME: Signed and Encrypted, RFC1847
Mission Specific	MIME encapsulation of EDI Objects, RFC 1767 MIME encapsulation of Macintosh files, RFC 1740 X.400/MIME Body Equivalences, RFC1494 MHS/RFC-822 Message Body Mapping, RFC1495 Mapping Between X.400 (1988), RFC 1327 X.400 Use of Extended Character Sets, RFC 1502 Postmaster Convention X.400 Operations, RFC 1648	SMTP 521 Reply Code, RFC1846 SMTP Service Extensions for Checkpoint/Restart, RFC1845 SMTP Service Ext. Large and Binary MIME Msgs., RFC1830

B.6. Network Applications, World Wide Web

	Mission Integration	Development
Global	Hypertext Markup Language - 2.0, RFC 1866 Form-based File Upload in HTML, RFC 1867 Relative Uniform Resource Locators, RFC1808 Standard Generalized Markup Language (SGML), FIPS PUB 152	The Secure HyperText Transfer Protocol (DRAFT) Use of the GSS-API for Web Security (DRAFT)
Mission Specific	N/A	N/A

B.7. Data Management

	Mission Integration	Development
Global	Database Languages -- SQL, ISO/IEC 9075:1992 Database Language SQL, ANSI X3.135-1992 Database Languages - SQL - Part 3: SQL Call Level Interface (SQL/CLI), ISO/IEC DIS 9075-3 The Object Database Management Standard: ODMG-93 , ed. by R. Cattell, Morgan Kaufmann Publishers, 1994	FIPS PUB 151-2, Portable Operating System Interface (POSIX) - System Applications Program Interface [with C language bindings] (ISO/IEC 9945-1:1990, POSIX.1) Microsoft Corporation Windows NT Systems Developer Kit (SDK)
Mission Specific	(Specific Vendors)	Information Builders, Inc., Enterprise Data Access/SQL (EDA/SQL) Sybase OmniSQL

B.8. Data Interchange

	Mission Integration	Development
Global	ISO/IEC 10918:1994, Information Technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines CompuServe Inc., Graphics Interchange Format (GIF), Version 89a ISO/IEC 11172-1:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 1: Systems ISO/IEC 11172-2:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 2: Video ISO/IEC 11172-3:1993 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 3: Audio ISO/IEC 11172-4:1995 Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1.5 Mbit/s -- Part 4: Conformance testing ISO/IEC DTR 11172-5 Information technology -- Coding of moving pictures and associated	ANSI/IEEE Std 754-1985, IEEE Standard for Binary Floating-Point Arithmetic ANSI X3.4-1986 (R1992), Coded Character Set 7-Bit American National Standard Code for Information Interchange ISO/IEC 646:1991, Information Technology -- ISO 7-bit coded character set for information interchange The Unicode Standard, Worldwide Character Encoding, Version 1.0, Volume 1, Addison-Wesley, 1990. The Unicode Standard, Worldwide Character Encoding, Version 1.0, Volume 2, Addison-Wesley, 1992. ISO/IEC 10646 -1:1993, Information technology -- Universal Multiple-Octet Coded Character Set Database Languages -- SQL, ISO/IEC 9075:1992 Database Language SQL, ANSI X3.135-1992 Database Languages - SQL - Part 3: SQL Call Level Interface (SQL/CLI), ISO/IEC DIS 9075-3 The Object Database Management

	audio for digital storage media up to about 1.5 Mbit/s -- Part 5: Software simulation National Space Sciences Data Center (NSSDC) Common Data Format (CDF) National Center for Supercomputing Applications (NCSA) Hierarchical Data Format (HDF) National Center for Atmospheric Research Network Common Data Format (netCDF) FIPS/PUB 128, Computer Graphics Metafile (CGM) International Astronomical Union Flexible Image Transfer Standard (FITS) World Meteorological Organization publication No. 306, Manual on Codes, Vol. 1, Part B, Secretariat of the WMO, Geneva, Switzerland, 1988, plus Supplements	Standard: ODMG-93 , ed. by R. Cattell, Morgan Kaufmann Publishers, 1994 CCSDS 620.0-B-2 Blue Book, Issue 2, Standard Formatted Data Units--Structure and Construction Rules, May 1992 CCSDS 630.0-B-1 Blue Book, Issue 1, Standard Formatted Data Units - Control Authority Procedures, June 1993 CCSDS 641.0-B-1 Blue Book, Parameter Value Language Specification (CCSD 00006(, May 1992 CCSDS 643.0-B-1 Blue Book, ASCII Encoded English (CCSD 0002), November 1992

B.9. Platform Portability

	Mission Integration	Development
Global	X/Open Publication Set T907, Single UNIX Specification, 1995 Draft Standard for Information Technology, X Window System Graphical User Interface - Part 1: Modular Toolkit Environment, IEEE Working Group P1295.1 FIPS PUB 158-1, User Interface Component of Applications Portability Profile (MIT X Window System) OSF Motif, Opens System Foundation, Motif Graphical User Interface X/Open Publication Set T408, XCDE Definitions, Infrastructure, Services and Applications Set FIPS PUB 151-2, Portable Operating System Interface (POSIX) - System Application Program Interface [with C language bindings], (also published as ISO/IEC 9945-1:1990, POSIX.1) FIPS PUB 189, Portable Operating System Interface (POSIX) - Part 2: Shell and Utilities, (also published as ISO/IEC 9945-	N/A

	2:1990, POSIX.2) IEEE 1003.1b-1993, Portable Operating System Interface (POSIX) - Part 1: System Application Program Interface (API) Amendment 1: Realtime Extension [C Language] IEEE Working Group P1003.6, POSIX - Security Extensions, IEEE 1003.1e and IEEE 1003.2c Microsoft Windows NT System Developer's Kit (SDK)	
Mission Specific	Apple Macintosh Windows 95	N/A

B.10. Languages

	Mission Integration	Development
Global	N/A	Goldberg, A. And Robson, D. Smalltalk-80: The Language. Reading, MA: Addison-Wesley, 1989. Goldberg, A. Smalltalk-80: The Interactive Programming Environment. Reading, MA: Addison-Wesley, 1984. ANSI X3J16/95-0088 and ISO WG21/N0688, April 1995 C++ Working Draft. Base documents are Stroustrup, B., The C++ Programming Language (Second Edition) (The Annotated Reference Manual), Addison-Wesley, 1991 and ISO/IEC 9899:1990, C Standard. FIPS PUB 119-1, Ada (ANSI/ISO/IEC 8652:1995) FIPS PUB 160, C (ANSI/ISO 9899:1992) FIPS PUB 69-1, Fortran (ANSI/X3.9-1978, ISO 1539:1980)
Mission Specific	N/A	Sun Microsystems, The Java Programmer's Guide Aho, A., Kernighan, B. , Weinberger, P., The AWK Programming Language. Addison-Wesley, 1988, ISBN-0-201-07981-X. Practical Extraction and Report Language (perl), Larry Walls, Documents freely available via many sites on WWW and Internet. Operating system specific shell languages (e.g., UNIX C Shell)

B.11. Development Tools

	Mission Integration	Development
Global	N/A	ISO/IEC 13719, Portable Common Tool Environment (PCTE) Application Programmer's Interface X/Open Publication Set T408, XCDE Definitions, Infrastructure, Services and Applications Set Windows 95 CDIF 1994 Interim Standard, consisting of Overview (EIA/IS-106, ISBN 0-7908-0012-8), Framework for Modeling and Extensibility (EIA/IS-107, ISBN 0-7908-0013-6), General Rules for Syntaxes and Encodings (EIA/IS-108, ISBN 0-7908-0014-4), SYNTAX.1 (EIA/IS-109, ISBN 0-7908-0015-2), ENCODING.1, (EIA/IS-110, ISBN 0-7908-0016-0), Foundation (EIA/IS-111, ISBN 0-7908-0017-9)
Mission Specific	N/A	N/A

Acronyms and Abbreviations

10Base-T	Communication standard: 10 megabits per second, Baseband, Twisted pair
ANSI	American National Standards Institute
AOS	Advanced Orbiting Systems
API	Application Program Interface
APP	Application Portability Profile
ARP	Address Resolution Protocol (IETF)
AWK	UNIX programming language, by Aho, Weinberger and Kernighan
BMP	Windows Bitmap file format
CARDS	Comprehensive Approach to Resusable Defense Software
CBC	Cipher Block Chaining
CCB	Configuration Control Board
CCITT	International Consultative Committee for Telephony and Telegraphy
CCR	Configuration Change Request
CCSDS	Consultative Committee for Space Data Systems
CDE	Common Desktop Environment
CDF	Common Data Format
CDIF	Case Data Interchange Format
CDRL	Contract Data Requirements List
CGM	Computer Graphics Metafile
CLI	Call-Level Interface
CMIP	Common Management Information Protocol
CORBA	Common Object Request Broker Architecture
COSE	Common Open Software Environment
CSL	Computer Systems Laboratory (NIST)
DBMS	Database Management System
DCE	Distributed Computing Environment
DCN	Document Change Notice
DES	Data Encryption Standard
DFS	Distributed File System
DIS	draft International Standard (ISO)
DISA	Defense Information Systems Agency
DNS	Domain Naming System
DSS	Digital Signature Standard (NIST standard)
DTR	Draft Technical Report
DTS	Distributed Time Service
DoD	Department of Defense
EDA	Enterprise Data Access
EDI	Electronic Data Interchange
Email	Electronic Mail

ESP	Encapsulating Security Payload (IETF)
Ethernet	Communication protocol
FDDI	Fiber Distributed Data Interface
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GIF	Graphics Interchange Format
GNMP	Government Network Management Protocol
GRIB	Gridded Binary (format)
GSFC	Goddard Space Flight Center
GSS	Generic Security Service (IETF)
HDF	Hierarchical Data Format
HIPPI	High Performance Parallel Interface
HST	Hubble Space Telescope
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IDEF0	Integration Definition for Function Modeling
IDEF1X	Integration Definition for Data Modeling
IDL	Interface Definition Language
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IPv6	Internet Protocol, version 6 (Current is v4)
ISDN	Integrated Services Digital Network (ISO/IEC standard)
ISO	International Organization for Standardization
ITU	International Telecommunications Union
JPEG	Joint Photographic Experts Group
JPL	Jet Propulsion Laboratory
JTC1	First Joint Technical Committee of ISO and IEC
Kbit/second	Kilobits per second
MD5	Message Digest 5, (IETF RFC 1321)
MHS	Message Handling System
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MIT	Massachusetts Institute of Technology
MMTF	Mobile Management Task Force
MO&DSD	Mission Operations and Data Systems Directorate
MPEG	Moving Picture Experts Group format
Mbit/second	Megabits per second
Msgs	Messages

NCSA	National Center for Supercomputing Applications
NDS	NetWare Directory Service
netCDF	Network Common Data Format
NFS	Network File System
NIST	National Institute for Standards and Technology
NSSDC	National Space Sciences Data Center
ODBC	Open Data Base Connectivity
ODMG	Object Data Management Group
OII	Open Information Interchange (European center)
OLE	Object Linking and Embedding
OMG	Object Management Group
ONC	Open Networking Computing (Sun Microsystems)
OODBMS	Object Oriented Database Management System
OQL	Object Query Language
OSF	Open Software Foundation
OSI	Open System Interconnection
OSPF	Open Shortest Path First routing
OSPF2	OSPF version 2
OTS	Off The Shelf
PARC	Palo Alto Research Center (Xerox)
PCTE	Portable Common Tools Environment
PEM	Privacy Enhanced Mail
perl	Practical Extraction and Report Language
POSIT	Profiles for Open Systems Internetworking Technologies
POSIX	Portable Operating System Interface
POSIX.1	POSIX Part 1, interfaces
POSIX.2	POSIX Part 2, shell and utilities
PPP	Point to Point Protocol (IETF)
RDBMS	Relational Database Management System
RF	Radio Frequency
RFC	Request For Comment
RIP2	Routing Information Protocol, version 2
RMON	Remote Network Monitoring (IETF)
RPC	Remote Procedure Call
RSA	RSA Data Security, Inc., holder of the encryption algorithm, and vendor
SC21	ISO/IEC JTC1 SubCommittee-21 on OSI, data management, et al.
SC22	ISO/IEC JTC1 SubCommittee-22 on programming languages and interfaces
SDH	Synchronous Digital Hierarchy
sed	stream editor (UNIX)
SFDU	Standard Formatted Data Unit
SGML	Standard Generalized Markup Language
SMI	Structure of Management Information
SMIv2	SMI version 2

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMPv1	SNMP version 1 (current standard)
SNMPv2	SNMP version 2 (proposed draft)
SONET	Synchronous Optical Network
SQL3	Structured Query Language, part 3 (Draft Standard)
SQL92	Structured Query Language (ANSI and ISO 1992 standard)
STARS	Software Technology for Adaptable, Reliable Systems (DoD)
STS	Space Transportation System
Sybase	Relational database management system vendor
TCP	Transmission Control Protocol
TFA	Transparent File Access
TP0	ISO/OSI data transport protocol
U.S.	United States
UDP	User Datagram Protocol
UNIX	Operating system name; rights now held by X/Open
VCDU	Virtual Channel Data Unit
WG21	JTC1/SC22 working group on C++, joint with ANSI
WG3	JTC1/SC21 working group on Database
WIN32	Microsoft Windows 32-bit application program interface
WMF	Windows Metafile format
WMO	World Meteorological Organization
WWW	World Wide Web
X3	Accredited Standards Committee (accredited by ANSI)
X3H2	Technical Committee on Database
X3J16	Technical Committee on Programming Language C++
X3J20	Technical Committee on Programming Language Smalltalk
X11R5	X-windows, Version 11, Release 5
XCDE	X/Open Common Desktop Environment standards
XDS	X/Open API to Directory Services
XMP	X/Open Management Protocols API
XMPP	X/Open Management Protocols Profile
XNFS	X/Open Network File System standards
XOM	X/Open OSI-Abstract-Data Manipulation API
XTI	X/Open Transport Interface

Glossary

Internet	The international network based on all using the Internet Protocols.
internet	Any network based on use of the Internet Protocols, whether a part of the Internet, or a private network
Internet Protocols	The suite of protocols standardized through the IETF.
internet protocol	The specific network layer protocol (IP) within the Internet Protocol suite.

Bibliography

NSI X3J16/95–0088 and ISO WG21/N0688, April 1995 C++ Working Draft. Base documents are: Stroustrup: *The C + + Programming Language* (second edition, Addison-Wesley Publishing Company, ISBN 0– 201– 53992– 6, copyright © 1991 AT&T) and ISO/IEC 9899:1990, *C Standard*.